Avira AntiVir Professional

User Manual

AVIRA®

Trademarks and Copyright

Trademarks

AntiVir is a registered trademark of Avira GmbH.
Windows is a registered trademark of the Microsoft Corporation in the United States and other countries.
All other brand and product names are trademarks or registered trademarks of their respective owners.
Protected trademarks are not marked as such in this manual. This does not mean, however that they may be used freely.

Copyright information

A code provided by a third party has been used for Avira AntiVir Professional. We thank the copyright owners for making the code available to us. For detailed information on copyright, please refer to in the help of Avira AntiVir Professional under the Third Party Licenses.

Table of Contents

1 Introduction 1

2 Icons and emphases 2

3 Product information 3

3.1 Delivery scope 3
3.2 System requirements 4
3.3 Licensing and Upgrade 5
3.3.1 License Manager 5

4 Installation and uninstallation 7

4.1 Installation 7
4.2 Modification installation 11
4.3 Installation modules 11
4.4 Uninstallation 12
4.5 Installation and uninstallation on the network 13
4.5.1 Installation on the network 14
4.5.2 Uninstallation on the network 14
4.5.3 Command line parameter for the setup program 15
4.5.4 Parameter of the file setup.inf 15

5 Overview of AntiVir Professional 19

5.1 User interface and operation 19
5.1.1 Control Center 19
5.1.2 Configuration 21
5.1.3 Tray icon 25
5.2 How to...? 26
5.2.1 Activate license 26
5.2.2 Avira AntiVir Professional automatic update 26
5.2.3 Start a manual update 28
5.2.4 On-demand scan: Using a scan profile to scan for viruses and malware 28
5.2.5 On-demand scan: Scan for viruses and malware using Dragamp;Drop 30
5.2.6 On-demand scan: Scan for viruses and malware via the context menu 30
5.2.7 On-demand scan: Automatically scan for viruses and malware 30
5.2.8 On-demand scan: Targeted scan for active rootkits 32
5.2.9 Reacting to detected viruses and malware 32
5.2.10 Quarantine: Handling quarantined files (*.qua) 36
5.2.11 Quarantine: Restore the files in quarantine 37
5.2.12 Quarantine: move suspicious files to quarantine 38
5.2.13 Scan profile: Amend or delete file type in a scan profile 39
5.2.14 Scan profile: Create desktop shortcut for scan profile 39
5.2.15 Events: Filter events 40
5.2.16 MailGuard: Exclude email addresses from scan 40
5.2.17 Firewall: Select the security level for the Firewall 41

6 Scanner::Overview 43

7 Updates 44

8 Avira Firewall::Overview 46

9 FAQ, Tips 47

9.1 Troubleshooting 47
9.2 Shortcuts 51
9.2.1 In dialog boxes 51
9.2.2 In the help 52
9.2.3 In the Control Center 52
9.3 Windows Security Center 54
9.3.1 General 54
9.3.2 The Windows Security Center and Avira AntiVir Professional 54

10 Viruses and more 57

10.1 Extended threat categories 57
10.2 Viruses and other malware 59

11 Info and Service 63

11.1 Contact address 63
11.2 Technical Support 63
11.3 Suspicious file 63
11.4 Reporting false positives 64
11.5 Your feedback for more security 64

12 Reference: Configuration options 65

12.1 Scanner 65
12.1.1 Scan 65
12.1.1.1. Action for concerning files 68
12.1.1.2. Further actions 70
12.1.1.3. Exceptions 72
12.1.1.4. Heuristic 73
12.1.2 Report 73
12.2 Guard 74
12.2.1 Scan 74
12.2.1.1. Action for concerning files 76
12.2.1.2. Further actions 79
12.2.1.3. Exceptions 80
12.2.1.4. Heuristic 83
12.2.2 ProActiv 83
12.2.2.1. Application filter: Applications to be blocked 84
12.2.2.2. Application filter: Permitted applications 85
12.2.3 Report 86
12.3 MailGuard 87
12.3.1 Scan 87
12.3.1.1. Action for concerning files 88
12.3.1.2. Other Actions 89
12.3.1.3. Heuristic 90
12.3.2 General 91
12.3.2.1. Exceptions 91
12.3.2.2. Cache 92
12.3.2.3. Footer 92
12.3.3 Report 93

12.4 Firewall 93
12.4.1 Adapter rules 94
12.4.1.1. Incoming Rules 96
12.4.1.2. Outgoing Rules 103
12.4.2 Application rules 103
12.4.3 Trusted vendors 106
12.4.4 Settings 107
12.4.5 Popup settings 108
12.5 Firewall under SMC 110
12.5.1 General settings 110
12.5.2 General adapter rules 111
12.5.2.1. Incoming Rules 113
12.5.2.2. Outgoing Rules 120
12.5.3 Application list 121
12.5.4 Trusted vendors 121
12.5.5 Additional settings 122
12.5.6 Display settings 123
12.6 WebGuard 124
12.6.1 Scan 124
12.6.1.1. Action for concerning files 125
12.6.1.2. Locked requests 127
12.6.1.3. Exceptions 128
12.6.1.4. Heuristic 131
12.6.2 Report 131
12.7 Update 132
12.7.1 Product update 133
12.7.2 Restart settings 134
12.7.3 File server 135
12.7.4 Web server 136
12.7.4.1. Proxy 137
12.8 General 137
12.8.1 Email 137
12.8.2 Extended threat categories 138
12.8.3 Password 139
12.8.4 Security 141
12.8.5 WMI 142
12.8.6 Directories 142
12.8.7 Warnings 143
12.8.7.1. Network 143
12.8.7.2. Email 145
12.8.7.3. Acoustic alerts 151
12.8.7.4. Warnings 152
12.8.8 Events 152
12.8.9 Limit reports 153

1 Introduction

Avira AntiVir Professional from Avira GmbH protects you computer against viruses, malware, adware and spyware, unwanted programs and other dangers. This manual deals with viruses and software in brief.

The manual describes the program installation and operation.

Please go to our website http://www.avira.com where you can download the Avira AntiVir Professional manual in PDF from, update Avira AntiVir Professional or renew your license.

You can also find information on our website such as telephone numbers for technical support and information on how to subscribe to our newsletter.

Your Avira GmbH team

2 Icons and emphases

The following icons are used:

Icon / Designation	Explanation
✓	Placed before a condition which must be fulfilled prior to implementation.
▸	Placed before an action step that you implement.
→	Placed before an event that follows the previous action.
Warning	Placed before a warning of the danger of critical data loss.
Note	Placed before a link to particularly important information or a tip which makes Avira AntiVir Professional easier to use.

The following emphases are used:

Emphasis	Explanation
Cursive	File name or path data.
	Displayed software interface elements (e.g. window heading, window field or options box).
Bold	Clicked software interface elements (e.g. menu item, section or button)

3 Product information

This chapter contains all information relevant to the purchase and use ofAvira AntiVir Professional:

- see chapter: Delivery scope
- see chapter: System requirements
- see chapter: Licensing
- see chapter: License Manager

Avira AntiVir Professional is a comprehensive and flexible tool you can rely on to protect your computer from viruses, malware, unwanted programs, and other dangers

▶ Please note the following information:

Note
Loss of valuable data usually has dramatic consequences. Even the best virus protection program cannot provide one hundred percent protection from data loss. Make regular copies (Backups) of your data for security purposes.

Note
A program can only provide reliable and effective protection from viruses, malware, unwanted programs and other dangers if it is up-to-date. Make sure Avira AntiVir Professional is up-to-date with automatic updates. Configure the program accordingly.

3.1 Delivery scope

Avira AntiVir Professional gives you the following functions:

- Control Center for monitoring, administering and controlling the entire program
- Central configuration with user-friendly standard and advanced options and context-sensitive help
- Scanner (On-Demand Scan) with profile-controlled and configurable scan for all known types of virus and malware
- Integration into the Windows Vista User Account Control allows you to carry out tasks requiring administrator rights
- Guard (On-Access Scan) for continuous monitoring of all file access attempts
- ProActive component for the permanent monitoring of program actions (for 32-bit system only, not available under Windows 2000)
- MailGuard (POP3 Scanner, IMAP Scanner and SMTP Scanner) for the permanent checking of emails for viruses and malware. Checking of email attachments is included
- WebGuard for monitoring data and files transferred from the Internet using the HTTP protocol (monitoring of ports 80, 8080, 3128)
- Integrated quarantine management to isolate and process suspicious files

- Rootkit protection for detecting hidden malware installed in your computer system (rootkits)
  (Not available under Windows XP 64 bit)
- Direct access to detailed information on the detected viruses and malware via the Internet
- Simple and quick updates to the program, virus definitions, and search engine through Single File Update and incremental VDF updates via a web server on the Internet or an intranet
- User-friendly licensing in License Manager
- Integrated Scheduler for planning one-off or recurring jobs such as updates or scans
- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method
- Detection of all conventional archive types including detection of nested archives and smart extension detection
- High-performance multithreading function (simultaneous high-speed scanning of multiple files)
- AntiVir Firewall for protecting your computer from unauthorized access from the Internet or another network and from unauthorized access to the Internet/network by unauthorized users.

3.2 System requirements

For Avira AntiVir Professional to work perfectly, the computer system must fulfill the following requirements:

- Computer as from Pentium, at least 266 MHz
- Operating system
- Windows 2000, SP4 and update rollup 1 or
- Windows XP, SP2 (32 or 64 Bit) or
- Windows Vista (32 or 64 Bit, SP 1 recommended)
- Windows 7 (32 or 64 Bit)
- At least 100 MB of free hard disk memory space (more if using Quarantine for temporary storage)
- At least 192 MB RAM under Windows 2000/XP
- At least 512 MB RAM under Windows Vista
- For the installation of Avira AntiVir Professional: Administrator rights
- For all installations: Windows Internet Explorer 6.0 or higher
- Internet connection where appropriate (see Installation)

Information for Windows Vista users

On Windows 2000 and Windows XP, many users work with administrator rights. However, this is not desirable from the point of view of security, because it is then easy for viruses and unwanted programs to infiltrate computers.

For this reason, Microsoft is introducing the "User Account Control" with Windows Vista. This offers more protection for users who are logged in as administrators: thus in Windows Vista, one administrator only has the privileges of a normal user at first. Actions for which administrator rights are required are clearly marked in Windows Vista with an information icon. In addition, the user must explicitly confirm the required action. Privileges are only increased and the administrative task carried out by the operating system after this permission has been obtained.

Avira AntiVir Professional requires administrator rights for some actions in Windows Vista. These actions are marked with the following symbol: . If this symbol also appears on a button, administrator rights are required to carry out this action. If your current user account does not have administrator rights, the Windows Vista dialog of the User Account Control asks you to enter the administrator password. If you do not have an administrator password, you cannot carry out this action.

3.3 Licensing and Upgrade

In order to be able to use Avira AntiVir Professional, you require a license. You thereby accept the license conditions of Avira AntiVir Professional.

The license is issued via a digital license code in the form of the file hbedv.key. This digital license code is the key to your personal license. It contains exact details of which programs are licensed to you and for what period of time. A digital license code can therefore also contain the license for more than one product.

If you purchased AntiVir Professional on the Internet, or via a program Avira AntiVir Professional CD/DVD, the digital license code is sent to you by email. You can load the license key during installation of AntiVir Professional or install it later in License Manager.

3.3.1 License Manager

The Avira AntiVir Professional License Manager enables very simple installation of the Avira AntiVir Professional license.

Avira AntiVir Professional License Manager

Avira AntiVir Professional License Manager
Avira AntiVir Professional
AVIRA
The selected file is an Avira AntiVir Professional license key file.
You can now install this license into your Avira AntiVir Professional product. Please select the apropriate Avira AntiVir Professional installation into which you would like to have this license installed and click OK.
Note: only those local Avira AntiVir Professional products for which this license key file contains a valid license are displayed.
License
Valid until
Destination Directory
Avira AntiVir Professional
31.12.2010
C:\Program Files\Avira\AntiVir
OK
Cancel

You can install the license by selecting the license file in your file manager or in the activation email with a double click and following the relevant instructions on the screen.

Note
The Avira AntiVir Professional License Manager automatically copies the corresponding license in the relevant product folder. If a license already exists, a note appears as to whether the existing license file is to be replaced. The existing file is then renamed (hbedv.old).

4 Installation and uninstallation

This chapter contains information relating to the installation and uninstallation of your Avira AntiVir Professional:

- see Chapter Installation: Conditions, Installation types, Install
- see Chapter Installation modules
- see Chapter Modification installation
- Installation and uninstallation on the network
- see Chapter Uninstallation: Uninstall

4.1 Installation

Before installing Avira AntiVir Professional, check whether your computer fulfils all the minimum system requirements. If your computer satisfies all requirements, you can install Avira AntiVir Professional.

Note
From Windows XP, Avira AntiVir Professional generates a restore point of your computer before installation of Avira AntiVir Professional. This enables you to safely remove Avira AntiVir Professional if installation fails. Note that for this the option **Turn off System Restore** under: "Start | Settings | Control Panel | System | Tab System Restore" must not be marked.
If you want to recover your system earlier, you can do so with the function "Start | Programs | Accessories | System Tools | System Restore". The restore point generated by Avira AntiVir Professional is indicated by the entry AntiVir Professional.

Installation types

During installation you can select a setup type in the installation wizard:

Express

- AntiVir Professional is completely installed with all program components.
- The program files are installed into a given standard folder under `C:\Program Files`.
- AntiVir Professional is installed with default settings. You have the option of defining custom settings using the configuration wizard.

User-defined

- You can choose to install individual program components (see Chapter Installation and uninstallation::Installation modules).
- A target folder can be selected for the program files to be installed.
- You can disable Create a desktop icon and program group in the Start menu.
- Using the configuration wizard, you can define custom settings for AntiVir Professional and initiate a short system scan which is carried out automatically after installation.

Before starting installation

- Close your email program. It is also recommended to end all running applications.
- Make sure that no other virus protection solutions are installed. The automatic protection functions of various security solutions may interfere with each other.
- Establish an Internet connection: The Internet connection is necessary for performing the following installation steps:
- Downloading the current program file and search engine, and the latest virus definition files via the installation program (for internet-based installation)
- Where appropriate, carrying out a AntiVir Professional update after completed installation
- Save the license file hbedv.key on your computer system, if you want to activate Avira AntiVir Professional.

Note
Internet-based installation:
Avira GmbH provides an installation program for the internet-based installation of Avira AntiVir Professional, which loads the current program file prior to installation by the Avira GmbH web servers. This process ensures that AntiVir Professional is installed with the latest virus definition file.
Installation with an installation package:
The installation package contains both the installation program and all necessary program files. No language selection for AntiVir Professional is available for installation with an installation package. We recommend that you carry out an update of the virus definition file after installation.

Install

The installation program runs in self-explanatory dialog mode. Every window contains a certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions:

- **OK:** Confirm action.
- **Abort:** Abort action.
- **Next:** Go to next step.
- **Back:** Go to previous step.

How to install AntiVir Professional:

Note
The following actions for disabling the Windows Firewall only apply to the Windows XP operating system.

- Start the installation program by double-clicking on the installation file you have downloaded from the Internet or insert the program CD.

Internet-based installation

→ The dialog box *Welcome...* appears.

- Click **Next** to continue with the installation.

→ The dialog box *Language selection* appears.

- Select the language you want to use to install AntiVir Professional and confirm your language selection by clicking **Next**.

➔ The dialog box *Download* appears. All files necessary for installation are downloaded by the Avira GmbH web servers. The *Download* window closes after conclusion of the download.

Installation with an installation package

➔ The installation wizard opens with the dialog box *Avira AntiVir Professional*.

▶ Click *Accept* to begin the installation.

➔ The installation file is extracted. The installation routine is started.

➔ The dialog box *Welcome...* appears.

▶ Click **Next**.

Continuing internet-based installation and installation with an installation package

➔ The dialog box with the license agreement appears.

▶ Confirm that you accept the license agreement and click **Continue**.

➔ The dialog box *Generate serial number* appears.

▶ Where appropriate, confirm that a random serial number has been generated and transmitted during update, and click **Continue**.

➔ The dialog box *Select installation type* appears.

▶ Decide whether you want to perform an express installation or a user-defined installation.

▶ Enable the option **Express** or**User-defined** and confirm by clicking **Continue**.

User-defined installation

➔ The dialog box *Select destination directory* appears.

▶ Confirm the specified destination directory by clicking **Continue**.

- OR -

Use the **Browse** button to select a different destination directory and confirm by clicking **Next**.

➔ The dialog box *Install components* appears:

▶ Enable or disable the required components and confirm by clicking **Continue**.

➔ If Windows Firewall is installed, a message appears indicating it must be disabled to avoid conflicts with the Avira Firewall.

▶ Click **Yes** to confirm.

➔ Windows Firewall is disabled.

➔ In the following dialog box you can decide whether to create a desktop shortcut and/or a program group in the Start menu.

▶ Click **Next**.

▶ Skip the following section "Express installation".

Express installation

➔ If Windows Firewall is installed, a message appears indicating it must be disabled to avoid conflicts with the Avira Firewall.

▶ Click **Yes** to confirm.

➔ Windows Firewall is disabled.

Resume: Express installation und user-defined installation

→ The dialog box *Install license* appears:

▶ Go to the directory in which you have saved the license file, read the message in the dialog box and confirm by clicking **Next**.

→ The license file is copied and the components are installed and started.

→ In the following dialog box you can choose whether to open the Readme file after installation is completed and whether to restart your computer.

▶ Agree where appropriate and complete the installation by clicking *Finish*.

→ The installation wizard is closed.

Resume: User-defined installation
Configuration wizard

→ If you choose user-defined installation, the following step opens the configuration wizard. The configuration wizard enables you to define custom settings for AntiVir Professional.

▶ Click **Next** in the welcome window of the configuration wizard to begin configuration of AntiVir Professional.

→ The *Configure AHeAD* dialog box enables you to select a detection level for the AHeAD technology. The detection level selected is used for the Scanner (On-demand scan) and Guard (On-access scan) AHeAD technology settings.

▶ Select a detection level and continue the installation by clicking **Next**.

→ In the following dialog box *Select extended threat categories*, you can adapt the protective functions of AntiVir Professional to the threat categories specified.

▶ Where appropriate, activate further threat categories and continue the installation by clicking *Next*.

→ If you have selected the AntiVir Firewall installation module, the*Firewall security level* dialog box appears. You can define whether the Avira Firewall should permit external access to enabled resources as well as network access by applications of trusted companies.

▶ Enable the required options and continue the configuration by clicking *Next*.

→ If you have selected the AntiVir Guard installation module, the*Guard start mode* dialog box appears. You can stipulate the Guard start time. At each computer reboot, the Guard will be started in the start mode specified.

Note
The specified Guard start mode is saved in the registry and cannot be changed via the Configuration.

▶ Enable the required option and continue the configuration by clicking *Next*.

→ In the following dialog box, *Select email settings*, you can define the server settings for sending email. AntiVir Professional uses SMPT to send emailssend email alerts.

▶ Where appropriate, make the necessary adjustments to the server settings and continue the configuration by clicking *Next*.

→ In the following dialog box, *System scan*, a short system scan can be enabled or disabled. The short system scan is carried out after the configuration has been completed and before the computer is rebooted, and scans running programs and the most important system files for viruses and malware.

- ▶ Enable or disable the *Short system scan* option and continue the configuration by clicking *Next*.

→ In the following dialog box, you can complete the configuration by clicking *Finish*

- ▶ Click *Finish* to complete the configuration.

→ The specified and selected settings are accepted.

→ If you have enabled the *Short system scan* option, the Luke Filewalker window opens. The Scanner performs a short system scan.

Resume: Express installation und user-defined installation

→ If you selected the **Restart computer** option in the final installation wizard, the computer reboots.

→ After the computer restart, the AntiVir Professional Readme file is displayed, if you selected the **Show Readme.txt** option in the installation wizard.

After a successful installation, we recommend that you check AntiVir Professional is up-to-date in the Control Center under *Overview :: Status*.

- ▶ Where appropriate, update AntiVir Professional to ensure the virus definition file is up-to-date.
- ▶ Then perform a full system scan.

4.2 Modification installation

You have the option of adding or removing individual program components of the current Avira AntiVir Professional installation (see ChapterInstallation and uninstallation::Installation modules)

If you wish to add or remove modules of the actual Avira AntiVir Professional installation, you can use the option **Add or Remove Programs** in the **Windows control panel** to **Change/Remove** programs.

Select Avira AntiVir Professional and click **Change**. In the welcome dialog of Avira AntiVir Professional select the option **Modify**. You will be guided through the installation changes.

4.3 Installation modules

In a user-defined installation or a modification installation, the following installation modules can be selected, added or removed.

- **AntiVir Professional**
  This module contains all components required for successful installation of Avira AntiVir Professional.

- **AntiVir Guard**
  The AntiVir Guard runs in the background. It monitors and repairs, if possible, files during operations such as open, write and copy in on-access mode. Whenever a user carries out a file operation (e.g. load document, execute, copy), Avira AntiVir Professional automatically scans the file. Renaming a file does not trigger a scan by AntiVir Guard.
- **AntiVir ProActiv**
  The ProActiv component monitors application actions and alerts users to application behavior typical of malware. This behavior-based recognition enables you to protect yourself against unknown malware. The ProActiv component is integrated into AntiVir Guard.
- **AntiVir MailGuard**
  MailGuard is the interface between your computer and the email server from which your email program (email client) downloads emails. MailGuard is connected as a so-called proxy between the email program and the email server. All incoming emails are routed through this proxy, scanned for viruses and unwanted programs and forwarded to your email program. Depending on the configuration, the program processes the affected emails automatically or asks the user for a certain action.
- **AntiVir WebGuard**
  When surfing the Internet, you are using your web browser to request data from a web server. The data transferred from the web server (HTML files, script and image files, Flash files, video and music streams, etc.) will normally be moved directly into the browser cache for display in the web browser, meaning that an on-access scan as performed by AntiVir Guard is not possible. This could allow viruses and unwanted programs to access your computer system. WebGuard is what is known as an HTTP proxy which monitors the ports used for data transfer (80, 8080, 3128) and scans the transferred data for viruses and unwanted programs. Depending on the configuration, the program may process the affected files automatically or prompt the user for a specific action.
- **Avira Firewall**
  Avira Firewall controls communication to and from your computer. It permits or denies communications based on security policies.
- ***AntiVir Rootkit Protection***
  AntiVir Rootkit Protection checks whether software is already installed on your computer that can no longer be detected with conventional methods of malware protection after penetrating the computer system.
- **Shell Extension**
  The Avira AntiVir Professional Shell Extension generates an entry in the context menu of the Windows Explorer (right-hand mouse button). Scan selected files with AntiVir. With this entry you can directly scan files or directories.

4.4 Uninstallation

If you wish to remove Avira AntiVir Professional from your computer, you can use the option **Add or Remove Programs** to **Change/Remove** programs in the Windows Control Panel.

To uninstall Avira AntiVir Professional (e.g. in Windows XP and Windows Vista):

- Open the **Control Panel** via the Windows **Start** menu.
- Double click on **Programs** (Windows XP: **Software**).
- Select **Avira AntiVir Professional** and click**Remove**.

→ You will be asked if you really want to remove the program.

→ You will be asked if you want to re-enable Windows Firewall (the Avira Firewall is disabled).

→ All components of the program are removed.

- Click on **Finish** to complete uninstallation.

→ Where appropriate, a dialog box appears recommending that your computer be restarted.

→ Avira AntiVir Professional is uninstalled, and all directories, files and registry entries for Avira AntiVir Professional are deleted when your computer is restarted.

4.5 Installation and uninstallation on the network

To simplify installation of Avira AntiVir Professional on a network of multiple client computers for the system administrator, Avira AntiVir Professional has a special procedure for the initial installation and the modification installation.

For automatic installation of Avira AntiVir Professional, the setup program works with the control file setup.inf. The setup program (presetup.exe) is contained in the Avira AntiVir Professional installation package. Installation is started with a script or batch file and all necessary information is obtained from the control file. The script commands therefore replace the usual manual inputs during installation.

Note
Please note that a license file is obligatory for initial installation on the network.

Note
Please note that a Avira AntiVir Professional installation package is required for installation via a network. An installation file for internet-based installation cannot be used.

Avira AntiVir Professional can be easily shared on the network with a server login script or via SMS.

For information on installation and uninstallation on the network:

- see Chapter: Command line parameter for the setup program
- see Chapter: Parameter of the file setup.inf
- see Chapter: Installation on the network
- see Chapter: Uninstallation on the network

Note
The AntiVir Security Management Center provides another easy option for the installation and uninstallation of Avira AntiVir Professional on the network. The AntiVir Security Management Center enables the remote installation and maintenance of AntiVir products on the network. For further information, please refer to our website http://www.avira.com.

4.5.1 Installation on the network

The installation can be script-controlled in batch mode.

The setup is suitable for the following installations

- Initial installation via the network (unattended setup)
- Installation on single-user computers

▶ Modification installation and update

Note
We recommend that you test automatic installation before the installation routine is implemented on the network.

To install Avira AntiVir Professional on the network automatically:

✓ You must have administrator rights (also required in batch mode)

▶ Configure the parameter of the file *setup.inf* and save the file.

▶ Begin installation of Avira AntiVir Professional with the parameter /inf or integrate the parameter into the login script of the server.

- Examples: `presetup.exe /inf="c:\temp\setup.inf"`

➔ The installation starts automatically.

4.5.2 Uninstallation on the network

To uninstall Avira AntiVir Professional on the network automatically:

✓ You must have administrator rights (also required in batch mode)

▶ Start the uninstallation of Avira AntiVir Professional with the parameter`/remsilent` or `/remsilentaskreboot` or integrate the parameter into the login script of the server.

You can also specify the parameter for the uninstallation log.

- Examples: `preetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

➔ The uninstallation starts automatically.

Note
The uninstallation setup program should be started on the PC on which AntiVir Professional is to be uninstalled; do not start the setup program from a network drive.

4.5.3 Command line parameter for the setup program

All path or file data must be placed in "...".

The following parameter is possible for installation:

– `/inf`

The setup program starts with the script mentioned and retrieves all parameters required.

Example: `presetup.exe /inf="c:\temp\setup.inf"`

The following parameters are possible for the uninstallation:

– `/remove`

The setup program uninstalls Avira AntiVir Professional.

Example: `presetup.exe /remove`

– `/remsilent`

The setup program uninstalls Avira AntiVir Professional without displaying dialogs. The computer is restarted after uninstallation.

Example: `presetup.exe /remsilent`

– `/remsilentaskreboot`

The set up program uninstalls Avira AntiVir Professional without displaying dialogs and requests a computer restart after uninstallation.

Example: `presetup.exe /remsilentaskreboot`

The following parameter is available as an option for the uninstallation log:

– `/unsetuplog`

All actions during uninstallation are logged.

Example: `preetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

4.5.4 Parameter of the file setup.inf

In the control file setup.inf, you can set the following parameters in the [DATA] field for the automatic installation of Avira AntiVir Professional. The sequence of the parameters is unimportant. If a parameter setting is missing or wrong, the setup routine is aborted and an error message is displayed.

– `DestinationPath`

Destination path, in which Avira AntiVir Professional is installed. It has to be included to the script. Please note that the setup includes company name and product name automatically. Environment variables can be used.

Example: DestinationPath=`%PROGRAMFILES%`
produces the installation path `C:\Programme\Avira\AntiVir Desktop`

– `ProgramGroup`

Creates a program group for all users of the computer in the Windows start menu.

`1`: Create program group

`0`: Do not create program group

Example: `ProgramGroup=1`

– `DesktopIcon`

Creates a shortcut desktop icon for all users of the computer on the desktop.

`1`: Create desktop icon

`0`: Do not create desktop icon

Example: `DesktopIcon=1`

– `ShellExtension`

Registers the shell extension in the registry. With the shell extension, files or directories can be scanned for viruses and malware via the context menu of the right-hand mouse button.

`1`: Register shell extension

`0`: Do not register shell extension

Example: `ShellExtension=1`

– `Guard`

Installs the AntiVir Guard (on-access scanner).

`1`: Install AntiVir Guard

`0`: Do not install AntiVir Guard

Example: `Guard=1`

– `MailScanner`

Installs the AntiVir MailGuard.

`1`: Install AntiVir MailGuard

`0`: Do not install MailGuard

Example: `MailScanner=1`

– `KeyFile`

Specify the path for the license file that is copied during installation. For initial installation: obligatory. The file name must be specified completely (fully qualified). (For a modification installation: optional.)

Example: `KeyFile=D:\inst\license\hbedv.key`

– `ShowReadMe`

Displays the readme.txt file after installation.

`1`: Display file

`0`: Do not display file

Example: `ShowReadMe=1`

– `RestartWindows`

Restarts the computer after installation. This entry has a higher priority than ShowRestartMessage.

`1`: Restart computer

`0`: Do not restart computer

Example: `RestartWindows=1`

– `ShowRestartMessage`

Displays information during the setup before carrying out an automatic restart.

`0`: Do not display information

`1`: Display information

Example: `ShowRestartMessage=1`

– `SetupMode`

Not required for initial installation. The setup program knows if an initial installation has been carried out. Specify the type of installation. If an installation is available already, it has to be indicated in the SetupMode whether this installation is an update only or a modification (reconfiguration) or an uninstallation.

`Update`: Updates an existing installation. In this case configuration parameters, for example Guard, are ignored.

`Modify`: Modifies (reconfigures) an existing installation. In the process no files are copied into the destination path.
`Remove`: Uninstalls AntiVir Professional from the system.

Example: `SetupMode=Update`

– `AVWinIni (optional)`

Specifies the destination path for the configuration file which may be copied during installation. The file name must be specified completely (fully qualified).

Example: `AVWinIni=d:\inst\config\avwin.ini`

– `Password`

This option assigns the password that was set for the (modification) installation and uninstallation to the setup routine. The entry is only scanned by the setup routine when a password has been set. If a password has been set and the password parameter is missing or wrong, the setup routine is aborted.

Example: `Password=Password123`

– `WebGuard`

Installs the AntiVir WebGuard.

`1`: Install AntiVir WebGuard

`0`: Do not install AntiVir WebGuard

Example: `WebGuard=1`

– `RootKit`

Installs the AntiVir rootkit protection module. Without AntiVir rootkit protection the scanner will not be able to scan for rootkits on the system!

`1`: Install AntiVir Rootkit Protection

`0`: Do not install AntiVir Rootkit Protection

Example: `RootKit=1`

– `HIPS`

Installs the AntiVir ProActive component. AntiVir ProActive is a pattern-based detection technology that enables as yet unknown malware to be detected.

`1`: Install ProActive

`0`: Do not install ProActive

Example: `HIPS=1`

– `Firewall`

Installs the Avira Firewall component. Avira Firewall monitors and controls the incoming and outgoing data traffic on your computer system and protects your computers from threats originating from the Internet or other network environments.

`1`: Install firewall

`0`: Do not install firewall

Example: `Firewall=1`

5 Overview of AntiVir Professional

This chapter contains an overview of the functionality and operation of AntiVir Professional.

- see Chapter Interface and operation
- see ChapterHow to...?

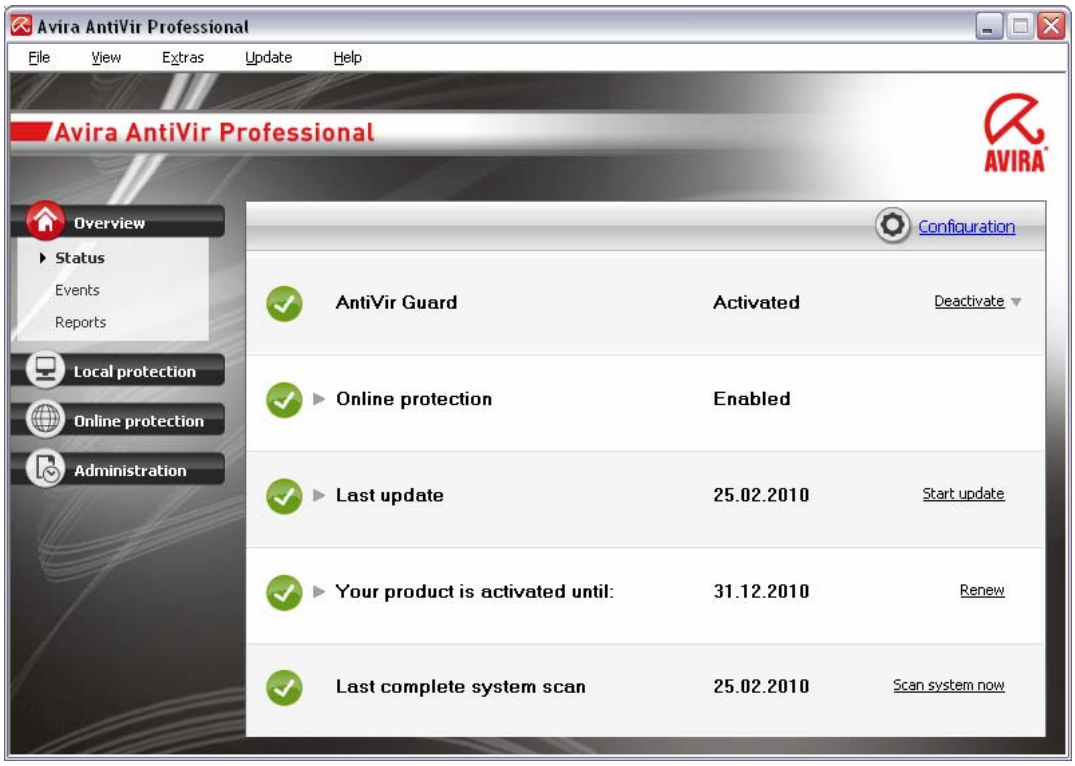
5.1 User interface and operation

Your operate AntiVir Professional via three program interface elements:

- Control Center: Monitoring and control of AntiVir Professional
- Configuration: Configuration of AntiVir Professional
- Tray Icon in the system tray of the taskbar: Open the Control Centre and other functions

5.1.1 Control Center

The Control Center is designed to monitor the protection status of your computer systems and control and operate the protection components and functions of AntiVir Professional.



The Control Center window is divided into three areas: the**menu bar**, the**navigation bar** and the detail window**view**:

- **Menu bar:** In the Control Center menu bar, you can access general program functions and information on AntiVir Professional.

- **Navigation area:** In the navigation area, you can easily swap between the individual sections of the Control Center. The individual sections contain information and functions of the program components of AntiVir Professional and are arranged in the navigation bar according to activity. Example: Activity *Overview* - Section**Status**.
- **View:** This window shows the section selected in the navigation area. Depending on the section, you will find buttons to execute functions and actions in the upper bar of the detail window. Data or data objects are displayed in lists in the individual sections. You can sort the lists by clicking in the box defining how you wish to sort the list.

Starting and closing of Control Center

To start the Control Center the following options are available:

- Double-click the program icon on your desktop
- via the AntiVir Professional program entry in the start menu | program.
- via the Avira AntiVir Professional tray icon.

Close the Control Center via the menu command **Close** in the menu **File** or by clicking on the close tab in the Control Center.

Operate Control Center

To navigate in the Control Center

▶ Select an activity in the navigation bar.

→ The activity opens and other sections appear. The first section of the activity is selected and displayed in the view.

▶ If necessary, click another section to display this in the detail window.

- OR -

▶ Select a section via the menu *View*.

Note
You can activate the keyboard navigation in the menu bar with the help of the [ALT] key. If navigation is activated, you can move within the menu with the arrow keys. With the Return key you activate the active menu item.
To open or close menus in the Control Center, or to navigate within the menus, you can also use the following key combinations: [Alt] + underlined letter in the menu or menu command. Hold down the [Alt] key if you want to access a menu, a menu command or a submenu.

To process data or objects displayed in the detail window:

▶ highlight the data or object you wish to edit.

To highlight multiple elements (elements in columns), hold down the control key or the shift key while selecting the elements.

▶ Click the appropriate button in the upper bar of the detail window to edit the object

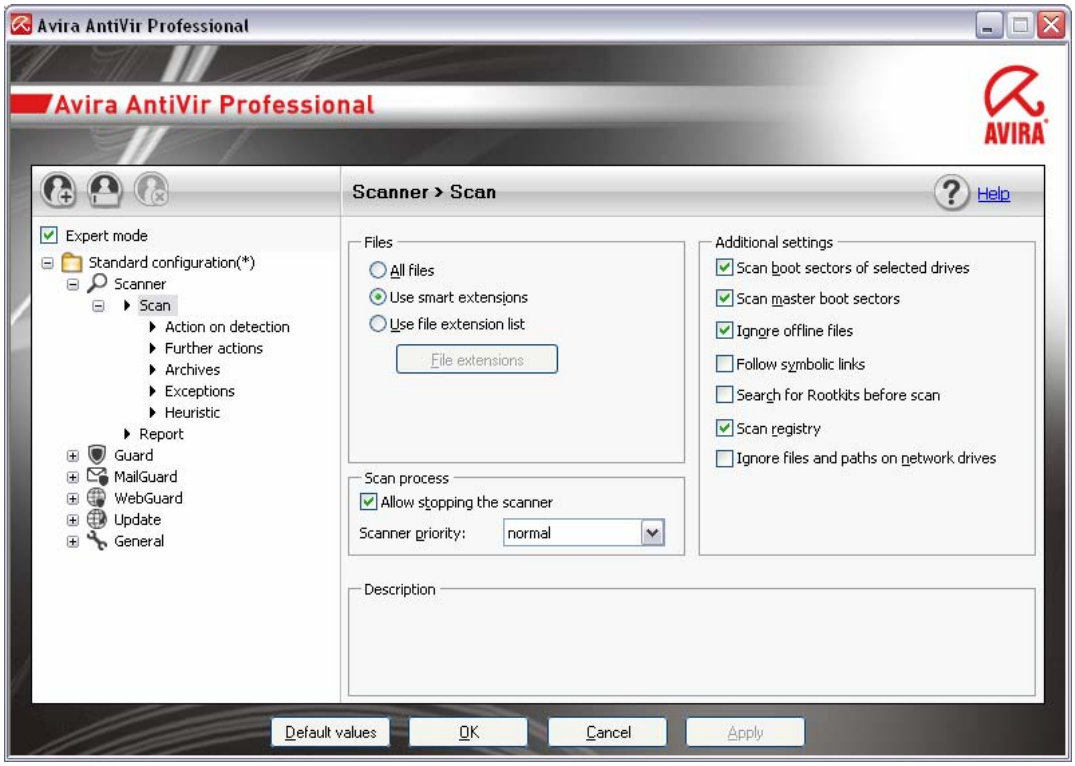
Control Center overview

- **Overview**: In **Overview** you will find all sections with which you can monitor the functioning of Avira AntiVir Professional.

- The **Status** section lets you see at a glance which Avira AntiVir Professional modules are active and provides information on the last update carried out. You can also see whether you own a valid license.
- The Events section enables you to view events generated by certain Avira AntiVir Professional modules.
- Die Reports section enables you to view the results of actions executed by Avira AntiVir Professional.
- **Local protection**: In**Local protection** you will find the components for checking the files on your computer system for viruses and malware.
- The Scan section enables you to easily configure and start an on-demand scan. Predefined profiles enable you to run a scan with preset default options. In the same way it is possible to adapt the scan for viruses and unwanted programs to your personal requirements with the help of manual selection (not saved) or by creating user-defined profiles, .
- The Guard section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
- **Online protection**: In **Online protection** you will find the components to protect your computer system against viruses and malware from the Internet, and against unauthorized network access.
- The MailGuard section shows you all the emails scanned by MailGuard, their properties and other statistical data.
- The WebGuard section shows you information on scanned URLs and detected viruses, as well as other statistical data, which can be reset at any time and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
- The Firewall section enables you to configure the basic settings for the Avira Firewall. In addition, the current data transfer rate and all active applications using a network connection are displayed.
- **Administration**: In **Administration** you will find tools for isolating and managing suspicious or infected files, and for planning recurring tasks.
- The Quarantine section contains the so-called Quarantine Manager. This is the central point for files already placed in quarantine or for suspect files which you would like to place in quarantine. It is also possible to send a selected file to the Avira Malware Research Center by email.
- The Scheduler section enables you to configure scheduled scanning and update jobs and to adapt or delete existing jobs.

5.1.2 Configuration

You can define AntiVir Professional settings in the Configuration. After installation, AntiVir Professional is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for AntiVir Professional may mean you need to adapt the protective components of AntiVir Professional.



The Configuration opens a dialog box: You can save your configuration settings via the OK or Accept buttons, delete you settings by clicking the Cancel button, or restore your default configuration settings using the Restore defaults button. You can select individual configuration sections in the left-hand navigation bar.

Accessing the AntiVir Professional Configuration

You have several options for accessing the configuration:

- via the Windows control panel.
- via the Windows Security Center - from Windows XP Service Pack 2.
- via the Avira AntiVir Professional tray icon.
- in the Avira AntiVir Professional Control Center via the menu item Extras | Configuration.
- in the Avira AntiVir Professional Control Center via the Configuration button.

Note
If you are accessing configuration via the **Configuration** button in the Control Center, go to the Configuration register of the section which is active in the Control Center. Expert mode must be activated to select individual configuration registers. In this case, a dialog appears asking you to activate expert mode.

Configuration operation

Navigate in the configuration window as you would in Windows Explorer:

- Click on an entry in the tree structure to display this configuration section in the detail window
- Click on the plus symbol in front of an entry to expand the configuration section and display configuration subsections in the tree structure.

▶ To hide configuration subsections, click on the minus symbol in front of the expanded configuration section.

Note
To enable or disable Configuration options and use the buttons, you can also use the following key combinations: [Alt] + underlined letter in the option name or button description.

Note
All configuration sections are only displayed in expert mode. Activate expert mode to view all configuration sections. Expert mode can be protected by a password which must be defined during activation.

If you want to confirm your Configuration settings:

▶ Click **OK**.

→ The configuration window is closed and the settings are accepted.

- OR -

▶ Click **Accept**.

→ The settings are accepted. The configuration window remains open.

If you want to finish configuration without confirming your settings:

▶ Click **Cancel**.

→ The configuration window is closed and the settings are discarded.

If you want to restore all configuration settings to default values:

▶ Click **Restore defaults**.

→ All settings of the configuration are restored to default values. All amendments and custom entries are lost when default settings are restored.

Configuration profiles

You have the option of saving your configuration settings as configuration profiles. In the configuration profile, i.e. of a configuration, all configuration options are saved in a group. The configuration is displayed in the navigation bar as a node. You can add other configurations to the default configuration. You can shift between configurations manually in the context menu of the tray icon. You also have the option of defining rules for switching to a specific configuration:
When switching configuration using a rule-based procedure, the configuration can be linked to the use of a LAN or Internet connection (identification via default gateway). In this way, configuration profiles can be created for different laptop usage scenarios:

- Use on company networks: Update via intranet server, WebGuard disabled
- Use at home: Update via default Avira GmbH web server, WebGuard enabled

You can add, rename, delete, copy or restore configurations and define rules for switching configurations using the buttons in the navigation bar, or using commands from the context menu in the configuration section.

Note
Automatic switching to another configuration is not supported in Windows 2000. No rules for switching configurations can be defined in Windows 2000.

Overview of configuration options

The following configuration options are available:

- **Scanner**: Configuration of on-demand scan

Scan options

Action on detections

File scan options

On-demand scan exceptions

On-demand scan heuristics

Report function setting

- **Guard**: Configuration of on-access scan

Scan options

Action on detections

On-access scan exceptions

On-access scan heuristics

Report function setting

- **MailGuard**: Configuration of MailGuard

Scan options: Enable the monitoring of POP3 accounts, IMAP accounts, outgoing emails (SMTP)

Actions on malware

MailGuard scan heuristics

MailGuard scan exceptions

Configuration of cache, empty cache

Configuration of a footer in sent emails

Report function setting

- **WebGuard**: Configuration of WebGuard

Scan options, enabling and disabling the WebGuard

Action on detections

Blocked access: Unwanted file types and MIME types, Web filter for known unwanted URLS (malware, phishing, etc.)

WebGuard scan exceptions: URLs, file types, MIME types

WebGuard heuristics

Report function setting

- **Firewall**: Configuration of the Firewall

Adapter rule setting

User-defined application rule settings

List of trusted producers (exceptions for network access by applications)

Expanded settings: Timeout for rules, lock Windows host file, stop Windows Firewall, notifications

Popup settings (alerts for network access by applications)

– **General**:

Configuration of email using SMTP

Extended risk categories for on-demand and on-access scan

Password protection for access to the Control Center and the Configuration

Security: Update status display, full system scan status display, product protection

WMI: Enable WMI support

Event log configuration

Configuration of report functions

Setting of directories used

Update: Configuration of connection to download server, download via Webserver or fileserver), set-up of product updates

Alerts: Configuration of email alerts for component(s):
Scanner
Guard
Updater
Configuration of network alerts for component(s) Scanner, Guard

Configuration of acoustic alerts when malware is detected

5.1.3 Tray icon

After installation, you will see the AntiVir Professional tray icon in the system tray of the taskbar:

Icon	Description
	AntiVir Guard is enabled and the Firewall is enabled
	AntiVir Guard is disabled and the Firewall is disabled

The tray icon displays the status of the AntiVir Guard service.

Central functions of Avira AntiVir Professional can be quickly accessed via the context menu of the tray icon. To open the context menu, click on the tray icon with the right-hand mouse button.

Entries in the context menu

– **Activate AntiVir Guard**: Enables or disables Avira AntiVir Guard.

– **Firewall**:

– Enable Firewall: enables/disables the Firewall

– Block all traffic: Enabled: Blocks all data transfers except transfers to the host computer system (Local Host/IP 127.0.0.1).

– Enable game mode: Enables or disables the mode:
Enabled: When activated, all defined adapter and application rules apply. Applications for which no rule is defined are permitted network access and no pop-up window is opened.

– **Start AntiVir**: Opens the Avira AntiVir Professional Control Center.

- **Configure AntiVir**: Opens the Configuration
- **Start update** Starts an update.
- **Help**: opens this online help.
- **Avira on the Internet**: Opens the web portal of AntiVir Professional on the internet. The condition for this is that you have an active connection to the Internet.

5.2 How to...?

5.2.1 Activate license

To activate the AntiVir Professional license:

Activate your license for Avira AntiVir Professional with the license file hbedv.key. You can get a license file from Avira GmbH by email. The license file contains the license for all products that you have ordered in one order process.

If you have not installed Avira AntiVir Professional yet:

- Save the license file to a local directory on your computer.
- Install Avira AntiVir Professional.
- During installation, enter the save location of the license file.

If you have installed Avira AntiVir Professional already:

- Double click on the license file in File Manager or in the activation email and follow the on-screen instructions when Avira AntiVir Professional License Manager opens.

  - OR -

- In the Avira AntiVir Professional Control Center, select the menu item Help / Load license file...

Note
In Windows Vista the User Account Control dialog box appears. Log in as administrator if appropriate. Click **Continue**.

- Highlight the license file and click **Open**.

→ A message appears.

- Click **OK** to confirm.

→ The license is activated.

- If necessary, restart your system.

5.2.2 Avira AntiVir Professional automatic update

To create a job with the AntiVir Scheduler to update Avira AntiVir Professional automatically:

- In the Control Center, select the **Management :: Scheduler** section.
- Click on the *Create new job with the wizard* icon.

→ The dialog box *Name and description of job* appears.

- Give the job a name and, where appropriate, a description.

→ The dialog box *Type of job* is displayed.

▶ Select **Update job** from the list.

→ The dialog box *Time of job* appears.

▶ Select a time for the update:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**
- **Login**

Note
We recommend that you update Avira AntiVir Professional regularly and often. The recommended update interval is: 60 minutes.

▶ Where appropriate, specify a date according to the selection.

▶ Where appropriate, select additional options (availability depends on type of job):

- **Also start job when Internet connection is established**

  In addition to the defined frequency, the job is carried out when an Internet connection is set up.

- **Repeat job if the time has already expired**

  Past jobs are carried out that could not be carried out at the required time, for example because the computer was switched off.

→ The dialog box *Select display mode* appears.

▶ Select the display mode of the job window:

- **Minimize**: progress bar only
- **Maximize**: Entire job window
- **Hide**: No job window

▶ Click **Finish**.

→ Your newly created job appears on the home page of the **Administration :: Scan** section as activated (check mark).

▶ Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:

View properties of a job

Modify job

Delete job

Start job

Stop job

5.2.3 Start a manual update

You have various options for starting an Avira AntiVir Professional update manually: When an update is started manually, the virus definition file and search engine are always updated. A product update can only take place if you have activated the option **Download and automatically install product updates** in the configuration under General :: Update

To start an Avira AntiVir Professional update manually:

- With the right-hand mouse button, click on the Avira AntiVir Professional tray icon in the taskbar.

→ A context menu appears.

- Select **Start update**.

→ The *Updater* dialog box appears.

- OR -

- In the Control Center, select the section **Overview :: Status**.
- In the *Last update* field, click on the **Start update** link.

→ The Updater dialog box appears.

- OR -

- In the Control Center, in the **Update** menu, select the menu command *Start update*.

→ The Updater dialog box appears.

Note
We strongly recommend regular automatic updates for Avira AntiVir Professional. The recommended update interval is: 60 minutes.

Note
You can also carry out a manual update directly via the Windows security centre.

5.2.4 On-demand scan: Using a scan profile to scan for viruses and malware

A scan profile is a set of drives and directories to be scanned.

The following options are available for scanning via a scan profile:

– Use predefined scan profile

if the predefined scan profile corresponds to your requirements.

– Customize and apply scan profile (manual selection)

if you want to scan with a customized scan profile.

– Create and apply new scan profile

if you want to create your own scan profile.

Depending on the operating system, various icons are available for starting a scan profile:

– In Windows XP and 2000:

This icon starts the scan via a scan profile.

– In Windows Vista:

In Microsoft Windows Vista, the control center at the moment only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the control centre with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

This icon starts a limited scan via a scan profile. Only directories and files that Windows Vista has granted access rights to are scanned.

This icon starts the scan with extended administrator rights. After confirmation, all directories and files in the selected scan profile are scanned.

To scan for viruses and malware with a scan profile:

- ▶ Go to Control Center and select the section **Local protection :: Scan**.
- → Predefined scan profiles appear.
- ▶ Select one of the predefined scan profiles.

  -OR-
- ▶ Adapt the scan profile *Manual selection*.

  -OR-
- ▶ Create a new scan profile
- ▶ Click on the icon (Windows XP: or Windows Vista:).
- ▶ The *Luke Filewalker* window appears and an on-demand scan is started.
- → When the scan is completed, the results are displayed.

If you want to adapt a scan profile:

- ▶ In the scan profile, expand **Manual Selection** the file tree so that all the drives and directories you want to scan are open.
  - – Click on the **+** symbol: The next directory level is displayed.
  - – Click on the **-** symbol: The next directory level is hidden.
- ▶ Highlight the nodes and directories you want to scan by clicking on the relevantbox of the appropriate directory level.

  The following options are available, Select directories:
  - – Directory, including sub-directories (black check mark)
  - – Directory excluding sub-directories (green check mark)
  - – Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
  - – No directory (no check mark)

If you want to create a new scan profile:

- ▶ Click on the **Create new profile** icon.
- → The profile *New profile* appears below the profiles previously created.
- ▶ Where appropriate, rename the scan profile by clicking on the icon .

- ▶ Highlight the nodes and directories to be saved by clicking on the check box of the respective directory level.

  The following options are available, Select directories:

  - Directory, including sub-directories (black check mark)
  - Directory excluding sub-directories (green check mark)
  - Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
  - No directory (no check mark)

5.2.5 On-demand scan: Scan for viruses and malware using Dragamp;Drop

To scan for viruses and malware systematically using Drag&Drop:

✓ The Avira AntiVir Professional Control Center has been opened.

- ▶ Highlight the file or directoryyou want to scan.
- ▶ Use the left-hand mouse button to drag the highlighted file or directory into the *Control Center*.

→ The *Luke Filewalker* window appears and an on-demand scan is started.

→ When the scan is completed, the results are displayed.

5.2.6 On-demand scan: Scan for viruses and malware via the context menu

To scan for viruses and malware systematically via the context menu:

- ▶ Click with the right-hand mouse button (e.g. in Windows Explorer, on the desktop or in an open Windows directory) on the file or directoryyou want to scan.

→ The Windows Explorer context menu appears.

- ▶ Select **Scan selected files with AntiVir** in the context menu.

→ The *Luke Filewalker* window appears and an on-demand scan is started.

→ When the scan is completed, the results are displayed.

5.2.7 On-demand scan: Automatically scan for viruses and malware

Note
After installation, the scan job *Full system scan* is created in the Scheduler: A full system scan is automatically carried out at a recommended interval.

To create a job to automatically scan for viruses and malware:

- ▶ In the Control Center, select the **Management :: Scheduler** section.
- ▶ Click on the icon

→ The dialog box *Name and description of job* appears.

- ▶ Give the job a name and, where appropriate, a description.

→ The dialog box *Type of job* appears.

▶ Select **Scan job**.

→ The dialog box *Select profile* appears.

▶ Select the profile to be scanned.

→ The dialog box *Time of job* appears.

▶ Select a time for the scan:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**
- **Login**

▶ Where appropriate, specify a date according to the selection.

▶ Where appropriate, select the following additional options (availability depends on job type):

- **Repeat job if the time has already expired**

  Past jobs are carried out that could not be carried out at the required time, for example because the computer was switched off.

→ The dialog box *Select display mode* appears.

▶ Select the display mode of the job window:

- **Minimize**: progress bar only
- **Maximize**: Entire job window
- **Hide**: No job window

▶ Select the *Shut down computer* option if you want the computer to shut down automatically when the scan is finished. This option is only available if the display mode is set to minimized or maximized.

▶ Click **Finish**.

→ Your newly created order appears as activated (check mark) on the homepage of the section *Administration :: Scheduler*.

▶ Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:

View properties of a job

Modify job

Delete job

Start job

Stop job

5.2.8 On-demand scan: Targeted scan for active rootkits

To scan for active rootkits, use the predefined scan profile *Scan for rootkits*.

To scan for active rootkits systematically:

- ▶ Go to Control Center and select the section **Local protection :: Scan**.
- → Predefined scan profiles appear.
- ▶ Select the predefined scan profile **Scan for active malware**.
- ▶ Where appropriate, highlight other nodes and directories to be scanned by clicking on the check box of the directory level.
- ▶ Click on the icon (Windows XP: or Windows Vista:).
- → The *Luke Filewalker* window appears and an on-demand scan is started.
- → When the scan is completed, the results are displayed.

5.2.9 Reacting to detected viruses and malware

For the individual protection components of AntiVir Professional, you can define how AntiVir Professional reacts to a detected virus or unwanted program in the Configuration under the section *Action for concerning files*.

No configurable action options are available for the ProActiv component of the Guard: Notification of a detection is always given in the *Guard: Suspicious application behavior* window.

Action options for the Scanner:

- – **Interactive**

  In interactive action mode, the results of the Scanner scan are displayed in a dialog box. This option is enabled as the default setting.
  In the case of **Scanner scan**, you will receive an alert with a list of the affected files when the scan is complete. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the Scanner.

- – **Automatic**

  In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically. If you enable the option *Display alert*, you will receive an alert whenever a virus is detected, indicating the action carried out.

Action options for the Guard:

- – **Interactive**

In interactive action mode, data access is denied and a desktop notification is displayed. In the desktop notification you can remove the malware detected or transfer the malware to the Scanner component using the Details button for further virus management. The Scanner opens a window containing notification of the detection, which gives you various options for managing the affected file via a context menu (see Detection::Scanner):

– **Automatic**

In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically. If you enable the option*Display alert*, you will receive a desktop notification whenever a virus is detected.

Action options for MailGuard, WebGuard:

– **Interactive**

In interactive action mode, if a virus or unwanted program is detected, a dialog box appears in which you can select what to do with the infected object. This option is enabled as the default setting.

– **Automatic**

In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically. If you enable the *Display alert* option, you will receive an alert when a virus is detected. The alert will allow you to confirm the action to be carried out.

In interactive action mode, you can react to detected viruses and unwanted programs by selecting an action for the infected object, displayed in the alert, and executing the selected action by clicking Confirm.

The following actions for handling infected objects are available for selection:

Note
Which actions are available for selection depends on the operating system, the protection components (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard) reporting the detection, and the type of malware detected.

Actions of the Scannerand the Guard (not ProActiv detections):

– **Repair**

The file is repaired

This option is only available if the infected file can be repaired.

– **Move to quarantine**

The file is packaged into a special format (**.qua*) and moved to the Quarantine directory *INFECTED* on your hard disk, so that direct access is no longer possible. Files in this directory can be repaired in Quarantine at a later data or, if necessary, sent to Avira GmbH.

– **Delete**

The file will be deleted. This process is much quicker than *overwrite and delete*. If a boot sector virus is detected, this can be deleted by deleting the boot sector. A new boot sector is written.

– **Overwrite and delete**

The file is overwritten with a default template and then deleted. It cannot be restored.

– **Rename**

The file is renamed with a **.vir* extension. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can be repaired and given their original name at a later time.

– **Ignore**

Avira AntiVir Professional takes no further action. The infected file remains active on your computer.

Warning
This could result in loss of data and damage to the operating system! Only select the *Ignore* option in exceptional cases.

– **Deny access**

Action option for Guard detections: Access to the infected file is blocked. The detection is only entered in the report file if the report function is enabled).

– **Copy to quarantine**

Action option for a rootkit detection: The detection is copied in quarantine.

– **Repair boot sector | Download repair tool**

Action options when infected boot sectors are detected: AntiVir Professional contains a number of options for repairing infected diskette drives. If AntiVir Professional is unable to perform the repair, you can download a special tool for detecting and removing boot sector viruses.

Note
If you carry out actions on running processes, the processes in question are terminated before the actions are carried out.

Actions of the Guard for detections made by the ProActiv component (notification of application actions typical of malware):

– **Trusted program**

The application continues to run. The program is added to the list of permitted applications and is excluded from monitoring by the ProActiv component. When adding to the list of permitted applications, the monitoring type is set to *Content*. This means that the application is only excluded from monitoring by the ProActiv component if the content remains unchanged (see Configuration::Guard::ProActiv::Application filter: Permitted applications).

– **Block program once**

The application is blocked, i.e. the application is terminated. The actions of the application continue to be monitored by the ProActiv component.

– **Always block this program**

The application is blocked, i.e. the application is terminated. The program is added to list of blocked applications and can no longer be run (see Configuration::Guard::ProActiv::Application filter: Applications to be blocked).

– **Ignore**

The application continues to run. The actions of the application continue to be monitored by the ProActiv component.

MailGuard actions: Incoming emails

– **Move to quarantine**

The email including all attachments is moved to quarantine. The affected email is deleted. The body of the text and any attachments of the email are replaced by a default text.

– **Delete**

The affected email is deleted. The body of the text and any attachments of the email are replaced by a default text.

– **Delete attachment**

The infected attachment is replaced by a default text. If the body of the email is affected, it is deleted and also replaced by a default text. The email itself is delivered.

– **Move attachment to quarantine**

The infected attachment is placed in quarantine and then deleted (replaced by a default text). The body of the email is delivered. The affected attachment can be delivered later by the quarantine manager.

– **Ignore**

The affected email is delivered.

Warning
This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore**option in exceptional cases. Disable the preview in your mail client, never open any attachments with a double click!

MailGuard actions: Outgoing emails

– **Move mail to quarantine (do not send)**

The email, together with all attachments, is copied to Quarantine and is not sent. The email remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

– **Block sending of mails (do not send)**

The email is not sent and remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

– **Ignore**

The affected email is sent.

Warning
Viruses and unwanted programs can penetrate the computer system of the email recipient in this way.

WebGuard actions:

– **Deny access**

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser.

– **Move to quarantine**

The website requested from the web server and/or any data or files transferred are moved to quarantine. The affected file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center.

– **Ignore**

The website requested from the web server and/or the data and files that were transferred are forwarded on by WebGuard to your web browser.

Warning
This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases.

Note
We recommend that you move any suspicious file that cannot be repaired to Quarantine.

Note
You can also send files reported by the heuristic to us for analysis.
For example, you can upload these files to our website:http://www.avira.com/sample-upload
You can identify files reported by the heuristic from the designation *HEUR/* or *HEURISTIC/* that prefixes the file name, e.g.: *HEUR/testfile.**.

5.2.10 Quarantine: Handling quarantined files (*.qua)

To handle quarantined files:

- In the Control Center, select the section **Administration :: Quarantine**.
- Check which files are involved, so that, if necessary, you can reload the original back onto your computer from another location.

If you want to see more information on a file:

- Highlight the file and click on

→ The dialog box *Properties* appears with more information on the file.

If you want to rescan a file:

Scanning a file is recommended if the Avira AntiVir Professional virus definition file has been updated and a false positive report is suspected. This enables you to confirm a false positive with a rescan and restore the file.

- Highlight the file and click on

→ The file is scanned for viruses and malware using the on-demand scan settings.

→ After the scan, the dialog *Scan statistics* appears which displays statistics on the status of the file before and after the rescan.

To delete a file:

- Highlight the file and click on .

If you want to upload the file to a Avira Malware Research Center web server for analysis:

- Highlight the file you want to upload.
- Click on

→ A dialog opens with a form for inputting your contact data.

- Enter all the required data.
- Select a type: **Suspicious file** or **False positive**.

▶ Click **OK.**

→ The file is uploaded to a Avira Malware Research Center web server in compressed form.

Note
In the following cases, analysis by the Avira Malware Research Center is recommended:
Heuristic hits (Suspicious file): During a scan, a file has been classified as suspicious by AntiVir Professional and moved to quarantine: Analysis of the file by the Avira Malware Research Center has been recommended in the virus detection dialog box or in the report file generated by the scan.
Suspicious file: You consider a file to be suspicious and have therefore moved this file to quarantine, but a scan of the file for viruses and malware is negative.
False positive: You assume that a virus detection is a false positive: AntiVir Professional reports a detection in a file, which is very unlikely to have been infected by malware.

Note
The size of the files you upload is limited to 20 MB uncompressed or 8 MB compressed.

Note
You can upload several files at once by selecting all the files you want to upload and then clicking the **Send Object** button.

If you want to copy a quarantined object from Quarantine to another directory:

▶ Highlight the quarantined object and click on

→ A scan dialog opens from which you can select a directory.

▶ Select a directory where you want to save a copy of the quarantined object and confirm your selection.

→ The selected quarantined object is saved to the selected directory.

Note
The quarantined object is not identical to the restored file. The quarantined object is encrypted and cannot be executed or read in its original format.

If you want to export the properties of a quarantined object in a text file:

▶ Highlight the quarantined object and click on

→ A text file opens containing the data from the selected quarantined object.

▶ Save the text file.

You can also restore the files in Quarantine:

– see Chapter: Quarantine: Restoring files in quarantine

5.2.11 Quarantine: Restore the files in quarantine

Different icons control the restore procedure, depending on the operating system:

– In Windows XP and 2000:

This icon restores the files to their original directory.

This icon restores the files to a directory of your choice.

– In Windows Vista:

In Microsoft Windows Vista, the control center at the moment only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the control centre with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

This icon restores the files to a directory of your choice.

This icon restores the files to their original directory. If extended administrator rights are necessary to access this directory, a corresponding request appears.

To restore files in quarantine:

Warning
This could result in loss of data and damage to the operating system of the computer! Only use the function *Restore selected object* in exceptional cases. Only restore files that could be repaired by a new scan.

✓ File rescanned and repaired.

▶ In the Control Center, select the section **Administration :: Quarantine**.

Note

Emails and email attachments can only be restored using the option and if they have the extension **.eml*.

To restore a file to its original location:

▶ Highlight the file and click on the (Windows 2000/XP: , Windows Vista). This option is not available for emails.

Note

Emails and email attachments can only be restored using the option and if they have the extension **.eml*.

→ A message appears asking if you want to restore the file.

▶ Click **Yes**.

→ The file is restored to the directory it was in before it was moved to quarantine.

To restore a file to a specified directory:

▶ Highlight the file and click on . .

→ A message appears asking if you want to restore the file.

▶ Click **Yes**.

→ The Windows default window for selecting the directory appears.

▶ Select the directory to restore the file to and confirm.

→ The file is restored to the selected directory.

5.2.12 Quarantine: move suspicious files to quarantine

To move a suspect file to quarantine manually:

▶ In the Control Center, select the section **Administration :: Quarantine**.

▶ Click on . .

→ The Windows default window for selecting a file appears.

▶ Select the file and confirm.

→ The file is moved to quarantine.

You can scan files in quarantine with the AntiVir Scanner:

- see Chapter: Quarantine: Handling quarantined files (*.qua)

5.2.13 Scan profile: Amend or delete file type in a scan profile

To stipulate additional file types to be scanned or exclude specific file types from the scan in a scan profile (only possible for manual selection and customized scan profiles):

✓ In the Control Center, go to the **Local protection ::** *Scan* section.

▶ With the right-hand mouse button, click on the scan profile you want to edit.

→ A context menu appears.

▶ Select **File filter**.

▶ Expand the context menu further by clicking on the small triangle on the right-hand side of the context menu.

→ The entries *Default*, *Scan all files* and *User-defined* appear.

▶ Select **User-defined**.

→ The *File extensions* dialog box appears with a list of all file types to be scanned with the scan profile.

If you want to exclude a file type from the scan:

▶ Highlight the file type and click **Delete**.

If you want to add a file type to the scan:

▶ Highlight the file type.

▶ Click **Add** and enter the file extension of file type into the input box.

Use a maximum of 10 characters and do not enter the leading dot. Wildcards (* and ?) are allowed as replacements.

5.2.14 Scan profile: Create desktop shortcut for scan profile

You can start an on-demand scan directly from your desktop via a desktop shortcut to a scan profile without accessing the Avira AntiVir Professional Control Center.

To create a desktop shortcut to the scan profile:

✓ In the Control Center, go to the **Local protection ::** *Scan* section.

▶ Select the scan profile you want to create a shortcut for.

▶ Click on the icon

→ The desktop shortcut is created.

5.2.15 Events: Filter events

Events that have been generated by AntiVir Professional program components are displayed in the Control Center under **Overview :: Events** (analogous to the event display of your Windows operating system). The program components are:

- Updater
- Guard
- MailGuard
- Scanner
- Scheduler
- FireWall

The following event types are displayed:

- Information
- Warning
- Error
- Detection

To filter displayed events:

- In the Control Center, select the section **Overview :: Results**.
- Check the box of the program components to display the events of the activated components.

  - OR -

  Uncheck the box of the program components to hide the events of the deactivated components.

- Check the event type box to display these events.

  - OR -

  Uncheck the event type box to hide these events.

5.2.16 MailGuard: Exclude email addresses from scan

To define which email addresses (senders) are excluded from the MailGuard scan (whitelisting):

- In the Control Center, select the section **Online protection:: MailGuard**.

→ The list shows incoming emails.

- Highlight the email you want to exclude from the MailGuard scan.
- Click on the appropriate icon to exclude the email from the MailGuard scan:

  In future, the selected email address will no longer be scanned for viruses and unwanted programs.

→ The email sender address is included in the exclusion list and no longer scanned for viruses, malware .

Warning
Only exclude email addresses from the MailGuard scan if the senders are completely trustworthy.

Note
Under MailGuard :: General :: Exceptions in the configuration, you can add more email addresses to the exclusion list or remove email addresses from the list.

5.2.17 Firewall: Select the security level for the Firewall

There are various security levels to choose from. Depending on which you choose, you have different adapter rule configuration options.

The following security levels are available:

- **Low**
- Flooding and port scan are detected.
- **Medium**
- suspicious TCP and UDP packages are discarded.
- Flooding and port scan are prevented.
- **High**
- Computer is not visible on the network.
- Connections from outside are blocked.
- Flooding and port scan are prevented.
- **User**
- User-defined rules: if this security level is selected, the program automatically recognizes that the adapter rules have been modified.

Note
The default security level setting for all predefined rules of the Avira Firewall is **High**

To define the security level for the Firewall:

▶ Go to Control Center and select the section Online **protection :: Firewall**.

▶ Move the slider to the required security level.

→ The selected security level is applied immediately.

6 Scanner::Overview

With the Scanner component, you can carry out targeted scans (on-demand scans) for viruses and unwanted programs. The following options are available for scanning for infected files:

- **On-demand scan via context menu**
  The on-demand-scan via the context menu (right-hand mouse button - entry **Scan selected files with AntiVir**) is recommended if, for example, you wish to scan individual files and directories. Another advantage is that it is not necessary to first start the Avira AntiVir Professional Control Center for an on-demand scan via the context menu.
- **On-demand scan via drag & drop**
  When a file or directory is dragged into the program window of the Avira AntiVir Professional Control Center, the Scanner scans the file or directory and all sub-directories it contains. This procedure is recommended if you wish to scan individual files and directories that you have saved, for example, on your desktop.
- On-demand scan via profiles
  This procedure is recommended if you wish to regularly scan certain directories and drives (e.g. your work directory or drives on which you regularly store new files). You do not then need to select these directories and drives again for every new scan, you simply select using the relevant profile.
- **On-demand scan via the Scheduler**
  The Scheduler enables you to carry out time-controlled scans.

Special processes are required when scanning for rootkits, boot sector viruses, and when scanning active processes. The following options are available:

- Scan for rootkits using the scan profile *Scan for active malware*
- Scan active processes via the scan profile *Active processes*
- Scan for boot sector viruses via the menu command **Scan for boot sector viruses** in the **Extras** menu

7 Updates

The effectiveness of anti-virus software depends on how up-to-date the program is, in particular the virus definition file and the search engine. To carry out updates, the Updater component is integrated into AntiVir Professional. The Updater ensures that Avira AntiVir Professional is always up-to-date and able to deal with the new viruses that appear every day. Updater updates the following components:

- Virus definition file:

  The virus definition file contains the virus patterns of the harmful programs used by AntiVir Professional to scan for viruses and malware and repair infected objects.

- Search engine:

  The search engine contains the methods used by AntiVir Professional to scan for viruses and malware.

- Program files (product update):

  Update packages for product updates make extra functions available to the individual program components.

An update checks whether the virus definition file and search engine are up-to-date and if necessary implements an update. Depending on the settings in the configuration, the Updater also carries out a product update or informs you of the product updates available. After a product update, you may have to restart your computer system. If only the virus definition file and search engine are updated, the computer does not have to be restarted.

Note
For security reasons, the Updater checks whether the Windows host file of your computer was altered to the effect that, for example, the Avira AntiVir Professional update URL was manipulated by malware and diverts the Updater to unwanted download sites. If the Windows host file has been manipulated, this is shown in the Updater report file.

AntiVir Professional is automatically updated in the following interval: 60 minutes. You can edit or disable the automatic update through the configuration (Configuration::Update).

In the Control Center under Scheduler, you can create additional update jobs that are carried out by Updater at the specified intervals. You also have the option to start an update manually:

- In the Control Center: in the Update menu and in the Status section
- via the context menu of the tray icon

Updates can be obtained from the Internet via a proprietary web server or via a web or file server on an intranet which downloads the update files from the Internet and makes them available to other computers on the network. This is useful if you want to update AntiVir Professional on multiple computers on a network. A download server on an intranet can be used to ensure AntiVir Professional is up-to-date on the protected computers using a minimum of resources. To set up a functioning download server on an intranet, you need a server which is compatible with the update structure of AntiVir Professional.

Note
You can use AntiVir Internet Update Manager (file server or web server in Windows) as a web server or file server in the intranet. AntiVir Internet Update Manager mirrors the download servers of Avira AntiVir products (including AntiVir Professional) and can be obtained on the Internet at http://www.avira.com.

When a web server is used, the HTTP protocol is used for the download. When using a file server, access to the update file is provided via the network. The connection to the web or file server is configured in the configuration under General :: Update. The default configuration uses the existing Internet connection as the connection to the Avira GmbH Web server.

8 Avira Firewall::Overview

Avira Firewall monitors and regulates incoming and outgoing data traffic on your computer system and protects you from a wide range of attacks and threats from the Internet: Based on security guidelines, incoming or outgoing data traffic or listening to ports will be allowed or denied. You will receive a desktop notification if Avira Firewall denies network activity and thus blocks network connections. The following options are available for Avira Firewall settings:

- by setting a security level in the Control Center

  You can define a security level in the Control Center. The *low*, *medium* and *high* security levels each contain several complementary security rules based on packet filters. These security rules are saved as predefined adapter rules in the Configuration under Firewall::Adapter rules.

- by saving actions in the Network Event window

  When an application first tries to create a network or Internet connection, the *Network Event* popup window appears. The *Network Event* window allows the user to choose whether the network activity of the application is allowed or denied. If the **Save Action for this application** option is enabled, the action is created as an application rule and is saved in the configuration under Firewall::Application Rules. Saving the actions in the Network Event window gives you a set of rules for the network activities of applications.

Note
For applications from trusted providers, network access is allowed by default, unless an adapter rule prohibits network access. You have the option of removing providers from the list of trusted providers.

- by creating adapter and application rules in the Configuration

  You can alter predefined adapter rules or create new adapter rules in the Configuration. The security level of the Firewall is automatically set to the value *User* if you add or change adapter rules.
  Application rules allow you to define monitoring rules specified for applications: You can use simple application rules to define whether all network activities of a software application are to be denied or allowed or whether they are to be handled by means of the *Network Event* popup window.
  In the advanced configuration of the *Application rules setting* you can define different packet filters for an application, which are executed as specified application rules.

Note
There are two different modes for application rules: *Privileged* and *Filtered*. For application rules in *filtered* mode, the relevant adapter rules are prioritized, i.e. relevant adapter rules are executed after the application rule. It is therefore possible that network access may be denied due to a high security level or corresponding adapter rules. For application rules in *privileged* mode, adapter rules are ignored. If applications are allowed in *privileged* mode, the application is always granted network access.

9 FAQ, Tips

This chapter provides a collection of frequently asked questions (FAQs) relating to Avira AntiVir Professional, a troubleshooting section and tips and tricks for using Avira AntiVir Professional.

see Chapter Troubleshooting

see Chapter Keyboard commands

see ChapterWindows Security Center

9.1 Troubleshooting

Here you will find information on causes and solutions of possible problems.

- The error message *The license file cannot be opened* appears.
- AntiVir MailGuard does not work.
- There is no network connection available in a virtual machine (e.g. VMWare, Virtual PC, ...) if Avira Firewall is installed on the host machine and the security level of Avira Firewall is set to medium or high.
- The Virtual Private Network (VPN) connection is blocked if the security level of Avira Firewall is set to medium or high.
- An email sent via a TSL connection has been blocked by MailGuard.
- Webchat is not operational: Chat messages will not be displayed

The error message *The license file cannot be opened* appears.

Reason: The file is encrypted.

▶ To activate the license, you do not need to open the file, but rather you save it in the program directory of Avira AntiVir Professional. See also Avira AntiVir Professional License administration.

The error message *Connection failed while downloading the file ...* appears when attempting to start an update.

Reason: Your Internet connection is inactive. This is why Avira AntiVir Professional cannot find the web server on the Internet.

▶ Test whether other Internet services such as WWW or email work. If not, reestablish the Internet connection.

Reason: The proxy server cannot be reached.

▶ Check whether the login for the proxy server has changed and adapt it to your configuration if necessary.

Reason: The update.exe file is not fully approved by your personal firewall.

▶ Ensure that the update.exe file is fully approved by your personal firewall.

Otherwise:

- Check your settings in the Configuration (expert mode) under General :: Update.

Viruses and malware cannot be moved or deleted.

Reason: The file was loaded by windows and is active.

- Update Avira AntiVir Professional.
- If you use the operating system Windows XP, deactivate System Restore.
- Start the computer in Safe Mode.
- Start Avira AntiVir Professional and the Configuration (expert mode).
- Choose Scanner :: Scan :: Files :: All files and confirm with **OK**.
- Start a scan of all local drives.
- Start the computer in Normal Mode.
- Carry out a scan in Normal Mode.
- If no other viruses or malware have been found, activate System Restore if it is available and to be used.

The status of the tray icon is disabled.

Reason: AntiVir Guard is disabled.

- In the Control Center in the section Overview :: Status in theAntiVir Guard panel, click on the **Enable** link.

Reason: AntiVir Guard is blocked by a firewall.

- Define a general approval for AntiVir Guard in the configuration of your firewall. AntiVir Guard only works with the address 127.0.0.1 (localhost). An Internet connection is not established. The same applies to AntiVir MailGuard.

Otherwise:

- Check the startup type of the AntiVir Guard service. If necessary, enable the service: In the taskbar, select "Start | Settings | Control Panel". Start the configuration panel "Services" with a double-click (under Windows 2000 and Windows XP the services applet is located in the sub-directory "Administrative Tools"). Find the entry "Avira AntiVir Guard". "Automatic" must be entered as the startup type and "Started" as the status. If necessary, start the service manually by selecting the relevant line and the button "Start". If an error message appears, please check the event display.

The computer is extremely slow when I perform a data back-up.

Reason: During the back-up procedure, AntiVir Guard scans all files being used by the back-up procedure.

- In the configuration (expert mode), choose Guard :: Scan :: Exceptions and enter the names of the backup software processes.

My Firewall reports AntiVir Guard and AntiVir MailGuard immediately after activation.

Reason: Communication with AntiVir Guardand AntiVir MailGuardoccurs via the TCP/IP Internet protocol. A firewall monitors all connections via this protocol.

▶ Define a general approval for AntiVir Guard and AntiVir MailGuard. AntiVir Guard only works with the address 127.0.0.1 (localhost). An Internet connection is not established. The same applies to AntiVir MailGuard.

AntiVir MailGuard does not work.

Please check correct functioning of AntiVir MailGuard with the aid of the following checklists if problems occur with AntiVir MailGuard.

Checklist

▶ Check whether your mail client logs in on the server via Kerberos, APOP or RPA. These verification methods are currently not supported.

▶ Check whether your mail client reports to the server through SSL (also often called TSL – Transport Layer Security). AntiVir MailGuard does not support SSL and therefore terminates any encrypted SSL connections. If you want to use encrypted SSL connections without having them protected by MailGuard, you will have to use a port that is not monitored by MailGuard for the connection. The ports monitored by MailGuard can be configured in the configuration under MailGuard::Scan.

▶ Is the AntiVir MailGuard service active? If necessary, enable the service: In the taskbar, select "Start | Settings | Control Panel". Start the configuration panel "Services" with a double-click (under Windows 2000 and Windows XP the services applet is located in the sub-directory "Administrative Tools"). Find the entry "Avira AntiVir MailGuard". "Automatic" must be entered as the startup type and "Started" as the status. If necessary, start the service manually by selecting the relevant line and the button "Start". If an error message appears, please check the event display. If this is not successful, you may have to completely uninstall Avira AntiVir Professional via "Start | Settings | Control Panel | Add or Remove Programs", restart the computer and then reinstall Avira AntiVir Professional.

General

▶ POP3 connections encrypted via SSL (Secure Sockets Layer, also frequently referred to as TLS (Transport Layer Security)) cannot currently be protected and are ignored.

▶ Verification to the mail server is currently only supported via "passwords". "Kerberos" and "RPA" are not currently supported.

▶ Avira AntiVir Professional does not check outgoing emails for viruses and unwanted programs.

Note
We recommend regularly installing Microsoft updates to close any gaps in security.

There is no network connection available in a virtual machine (e.g. VMWare, Virtual PC, etc.) if Avira Firewall is installed on the host machine and the security level of Avira Firewall is set to medium or high.

If Avira Firewall is installed on a computer on which a virtual machine (for example VMWare, Virtual PC, etc.) is also running, the firewall will block all network connections for the virtual machine when the security level of the Avira Firewall is set to medium or high. If the security level is set to low, the Firewall works as expected.

Reason: The virtual machine emulates through software a network card. This emulation encapsulates the data packages of the guest system in special packages (UDP packages) and routes them via the external gateway back to the host system. Avira Firewall rejects these packages coming from outside, starting from security level medium.

To avoid this behavior do the following:

- Go to Control Center and select the section **Online protection :: Firewall**.
- Click the **Configuration** link.
- The *Configuration* dialog box is displayed. You are in the configuration section *Application rules*.
- Activate the **Expert mode** option.
- Select the configuration section **Adapter rules**.
- Click **add rule**.
- Select **UDP** in the section *Incoming rules*.
- Type the **name** of the rule in the Section Name of the rule .
- Click **OK**.
- Check if the rule is directly above the rule **Deny all IP packets**.

Warning
This rule is potentially dangerous because it will allow UDP packets without any filtering! After working with the virtual machine change to your previous security level.

The Virtual Private Network (VPN) connection is blocked if the security level of Avira Firewall is set to medium or high.

Reason: This problem is caused by the last rule **Deny all IP packets** which discards all packets that do not comply with any of the rules above it. The type of packages dispatched by the VPN software (so-called GRE packets) do not fit into the other categories and therefore they are filtered by this rule.

Replace the rule **Deny all IP packets** with two new rules which will deny the TCP and UPD packets. In this way there is the possibility to allow packets of other protocols.

An email sent via a TSL connection has been blocked by MailGuard.

Reason: Transport Layer Security (TLS: encryption protocol for data transfers on the Internet) is not supported by MailGuard at this time. The following options are available for sending the email:

- Use a different port from port 25, which is used by SMTP. This will bypass monitoring by MailGuard.
- Turn off the TSL encrypted connection and disable TSL support in your email client.
- Disable (temporarily) monitoring of outgoing emails by MailGuard in the configuration under MailGuard::Scan.

Webchat is not operational: Chat messages are not displayed; data are being loaded in the browser.

This phenomenon may occur during chats, which are based on the HTTP protocol with 'transfer-encoding= chunked'.

Reason: WebGuard checks the data sent completely for viruses and undesired programs first of all, before the data are loaded into the web browser. During a data transfer with 'transfer-encoding= chunked', WebGuard cannot determine the message length or the data volume.

▶ Enter the configuration of the URL of the web chats as an exception (see Configuration: WebGuard::Exceptions).

9.2 Shortcuts

Keyboard commands - also called shortcuts - offer a fast possibility to navigate, to retrieve individual modules and to start actions through Avira AntiVir Professional.

Below we provide you with an overview of the available keyboard commands in Avira AntiVir Professional. Please find further indications regarding the functionality in the corresponding chapter of the help.

9.2.1 In dialog boxes

Shortcut	Description
Ctrl + Tab Ctrl + Page down	Navigation in the Control Center Go to next section.
Ctrl + Shift + Tab Ctrl + Page up	Navigation in the Control Center Go to previous section.
← ↑ → ↓	Navigation in the configuration sections First, use the mouse to set the focus on a configuration section.
Tab	Change to the next option or options group.
Shift + Tab	Change to the previous option or options group.
← ↑ → ↓	Change between the options in a marked drop-down list or between several options in a group of options.
Space	Activate or deactivate a check box, if the active option is a check box.
Alt + underlined letter	Select option or start command.
Alt + ↓ F4	Open selected drop-down list.
Esc	Close selected drop-down list. Cancel command and close dialog.
Enter	Start command for the active option or button.

9.2.2 In the help

Shortcut	Description
Alt + Space	Display system menu.
Alt + Tab	Shift between the help and the other opened windows.
Alt + F4	Close help.
Shift + F10	Display context menu of the help.
Ctrl + Tab	Go to next section in the navigation window.
Ctrl + Shift + Tab	Go to previous section in the navigation window.
Page up	Change to the subject, which is displayed above in the contents, in the index or in the list of the search results.
Page down	Change to the subject, which is displayed below the current subject in the contents, in the index or in the list of the search results.
Page up Page down	Browse through a subject.

9.2.3 In the Control Center

General

Shortcut	Description
F1	Display help
Alt + F4	Close Control Center
F5	Refresh
F8	Open configuration
F9	Start update

Scan section

Shortcut	Shortcut
F2	Rename selected profile
F3	Start scan with the selected profile
F4	Create desktop link for the selected profile
Ins	Create new profile
Del	Delete selected profile

Firewall section

Shortcut	Description
Return	Properties

Quarantine section

Shortcut	Description
F2	Rescan object
F3	Restore object
F4	Send object
F6	Restore object to...
Return	Properties
Ins	Add file
Del	Delete object

Scheduler section

Shortcut	Description
F2	Edit job
Return	Properties
Ins	Insert new job
Del	Delete job

Reports section

Shortcut	Description
F3	Display report file
F4	Print report file
Return	Display report
Del	Delete report(s)

Events section

Shortcut	Description
F3	Export event(s)
Return	Show event
Del	Delete event(s)

9.3 Windows Security Center

- Windows XP Service Pack 2 or higher -

9.3.1 General

The Windows Security Center checks the status of a computer for important security aspects.

If a problem is detected with one of these important points (e.g. an outdated anti-virus program), the Security Center issues an alert and gives recommendations on how to protect your computer better.

9.3.2 The Windows Security Center and Avira AntiVir Professional

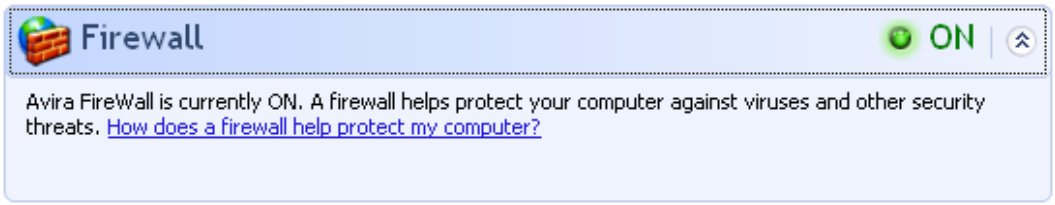
Firewall

You may receive the following information from the Security Center with regard to your firewall:

- Firewall ACTIVE / Firewall on
- Firewall INACTIVE / Firewall off

Firewall ACTIVE / Firewall off

After installation of Avira AntiVir Professional and turned off Windows Firewall, you receive the following message:


Firewall
ON
Avira FireWall is currently ON. A firewall helps protect your computer against viruses and other security threats. How does a firewall help protect my computer?

Firewall INACTIVE / Firewall off

You will receive the following message as soon as you disable the Avira Firewall:

Firewall
OFF
Avira FireWall reports that it is currently turned off. A firewall helps protect your computer from potentially harmful content on the Internet. Click Recommendations to learn how to fix this problem. How does a firewall help protect my computer?
Recommendations...

Note
You can enable or disable the Avira Firewall via the Status tab in the Avira AntiVir Professional Control Center.

Warning
If you turn the Avira Firewall off, your computer is no longer prevented by unauthorized users from gaining access to it through a network or the Internet.

Virus protection software / Protection against malicious software

You may receive the following information from the Windows Security Center with regard to your virus protection.

Virus protection NOT FOUND

Virus protection OUT OF DATE

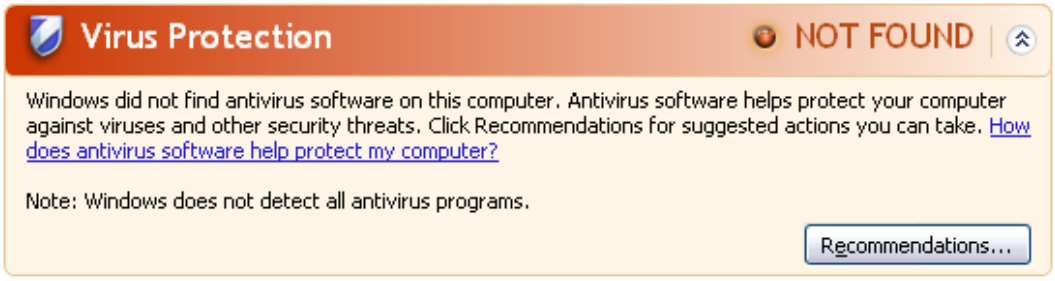
Virus protection ON

Virus protection OFF

Virus protection NOT MONITORED

Virus protection NOT FOUND

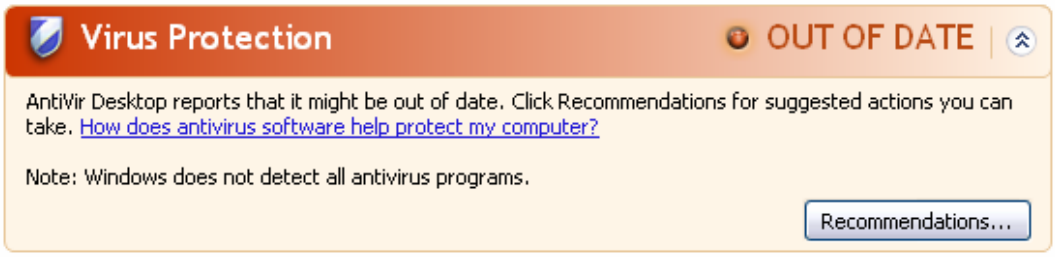
This information of the Windows Security Center appears when the Windows Security Center has not found any anti-virus software on your computer.


Virus Protection
NOT FOUND
Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?
Note: Windows does not detect all antivirus programs.
Recommendations...

Note
Install Avira AntiVir Professional on your computer to protect it against viruses and other unwanted programs!

Virus protection OUT OF DATE

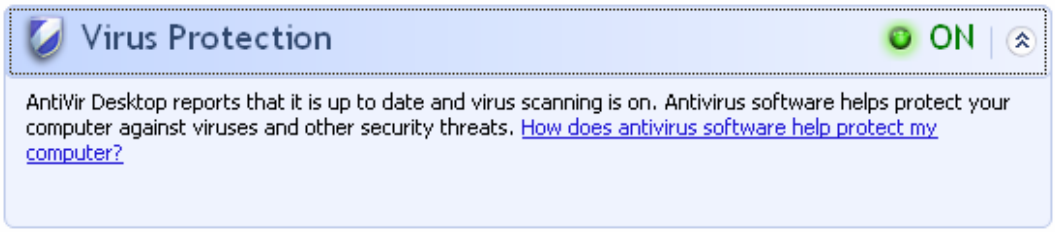
If you have already installed Windows XP Service Pack 2 or Windows Vista and then install Avira AntiVir Professional or you install Windows XP Service Pack 2 or Windows Vista on a system on which Avira AntiVir Professional has already been installed, you receive the following message:


Virus Protection
OUT OF DATE
AntiVir Desktop reports that it might be out of date. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?
Note: Windows does not detect all antivirus programs.
Recommendations...

Note
In order for the Windows Security Center to recognize Avira AntiVir Professional as up to date, an update must be carried out after installation. Update your system by carrying out an Avira AntiVir Professional update.

Virus protection ON

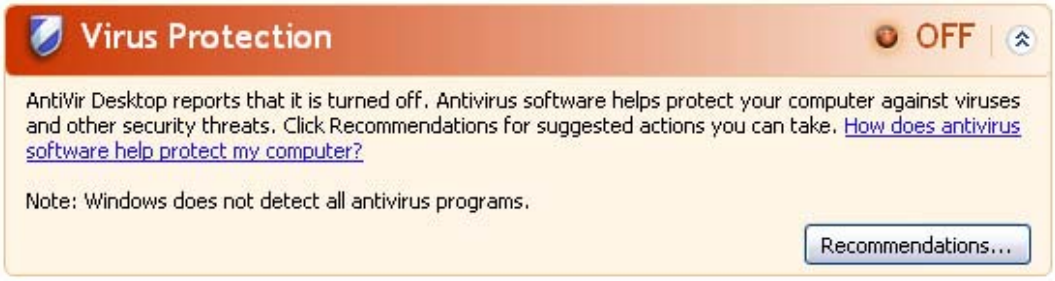
After installation of Avira AntiVir Professional and a subsequent update, you receive the following message:


Virus Protection
ON
AntiVir Desktop reports that it is up to date and virus scanning is on. Antivirus software helps protect your computer against viruses and other security threats. How does antivirus software help protect my computer?

Avira AntiVir Professional is now up to date and the AntiVir Guard is enabled.

Virus protection OFF

You receive the following message if you disable the AntiVir Guard or stop the Guard service.

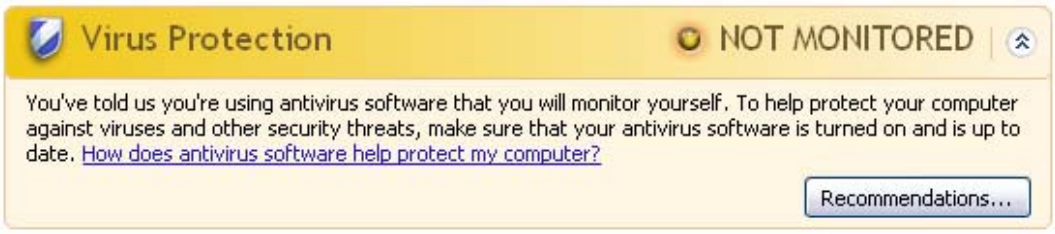

Virus Protection
OFF
AntiVir Desktop reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?
Note: Windows does not detect all antivirus programs.
Recommendations...

Note
You can enable or disabled AntiVir Guard in the Overview :: Status section of theAvira AntiVir Professional Control Center . You can also see that the AntiVir Guard is enabled if the red umbrella in your taskbar is open.

Virus protection NOT MONITORED

If you receive the following message from the Windows Security Center, you have decided that you want to monitor your anti-virus software yourself.

Note
This function is not supported by Windows Vista.


Virus Protection
NOT MONITORED
You've told us you're using antivirus software that you will monitor yourself. To help protect your computer against viruses and other security threats, make sure that your antivirus software is turned on and is up to date. How does antivirus software help protect my computer?
Recommendations...

Note
The Windows Security Center is supported by Avira AntiVir Professional. You can enable this option at any time via the button "Recommendations...".

Note
Even if you have installed Windows XP Service Pack 2 or Windows Vista, you still require a virus protection solution, e.g. Avira AntiVir Professional. Although Windows XP Service Pack 2 monitors your anti-virus software, it does not contain any anti-virus functions itself. Therefore you would not be protected against viruses and other malware without an additional anti-virus solution!

10 Viruses and more

10.1 Extended threat categories

Dialers (DIALERS)

Certain services available in the Internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the Internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask directly your telephone provider to block this number range to be immediately protected against undesired dialers (0190/0900 dialers).

Avira AntiVir Professional can detect the familiar dialers by default.

If the option **Dialers** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if a dialer is detected. You can now simply delete the potentially unwanted 0190/0900 dialer. However, if it is a wanted dial-up program, you can declare it an exceptional file and this file is then no longer scanned in future.

Games (GAMES)

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the Internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Avira AntiVir Professional detects computer games. If the **Games** option is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects a game. The game is now over in the truest sense of the word, because you can simply delete it.

Jokes (JOKES)

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Thanks to the extension of its scanning and identification routines, Avira AntiVir Professional is able to detect joke programs and eliminate them as unwanted programs if required. If the option **Jokes** is enabled with a check mark in the configuration under Extended threat categories, a corresponding alert is issued if a joke program is detected.

Security Privacy Risk (SPR)

Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.

Avira AntiVir Professional detects "Security Privacy Risk" software. If the option **Security Privacy Risk** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects such software.

Backdoor Clients (BDC)

In order to steal data or manipulate computers, a backdoor server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the Internet or a network.

Avira AntiVir Professional detects "backdoor control software". If the option **Backdoor Clients** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects such software.

Adware/Spyware (ADSPY)

"Software that displays advertising or software that sends the user's personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted."

Avira AntiVir Professional detects "Adware/Spyware". If the option **Adware/Spyware** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects such software.

Unusual Runtime Compression Tools (PCK)

Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

Avira AntiVir Professional detects "Unusual runtime Compression Tools". If the option **Unusual runtime Compression Tools** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects such packers.

Double Extension Files (HEUR-DBLEXT)

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Avira AntiVir Professional detects "Double Extension Files". If the option **Double Extension files** (HEUR-DBLEXT) is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects such files.

Phishing

Phishing, also known as *brand spoofing* is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.
When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

Avira AntiVir Professional detects "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Professional detects such behavior.

Application (APPL)

The term APPL refers to an application which may involve a risk when used or is of dubious origin.

Avira AntiVir Professional detects "Application (APPL)". If the option **Application (APPL)** is enabled with a check mark in the configuration under Extended threat categories , you receive a relevant alert if Avira AntiVir Professional detects such behavior.

10.2 Viruses and other malware

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Backdoors

A backdoor can gain access to a computer by circumventing computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help, but are mainly used to install further computer viruses or worms on the relevant system. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Boot viruses

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more&ldots;

Bot-Net

A bot net is defined as a remote network of PCs (on the Internet), which is composed of bots that communicate with each other. A Bot-Net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-Nets serve various purposes, including Denial-of-service attacks etc., partly without the affected PC user's knowledge. The main potential of Bot-Nets is that the networks can achieve dimensions on thousands of computers and its bandwidth sum bursts most conventional Internet accesses.

Exploit

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. A form of an exploit for example are attacks from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

Hoaxes

For several years, Internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread per email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

Honeypot

A honeypot is a service (program or server) installed in a network. It has the function to monitor a network and to protocol attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a Honeypot, it is logged and an alert is triggered.

Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses do consequently not attack executable files but they do attack the documents of the corresponding host-application.

Pharming

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

Phishing

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

Polymorph viruses

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

Program viruses

A computer virus is a program that is capable to attach itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits his virulent code. The program execution of the host itself is not changed as a rule.

Rootkit

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

Script viruses and worms

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms can consequently not form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

Spyware

Spyware are so-called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

Trojan horses (short Trojans)

Trojans are pretty common nowadays. We are talking about programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

Zombie

A Zombie-PC is a computer that is infected with malware programs and enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

11 Info and Service

This chapter contains information on how to contact us.

see Chapter Contact address

see Chapter Technical support

see Chapter Suspicious files

see Chapter Report false positives

see Chapter Your feedback for more security

11.1 Contact address

If you have any questions or requests concerning the Avira AntiVir Professional product range, we will be pleased to help you. You will find our contact addresses in the Control Center under Help :: About Avira AntiVir Professional.

11.2 Technical Support

Avira AntiVir Professional support provides reliable assistance in answering your questions or solving a technical problem.

All necessary information on our comprehensive support service can be obtained from our website http://www.avira.com/professional-support.

All necessary information on our comprehensive support service can be obtained from our website http://www.avira.com/professional-support.

- **License information**. This can be found on the program interface under the menu item Help :: About AntiVir Professional :: License information.
- **Version information**. This can be found on the program interface under the menu item Help :: About AntiVir Professional :: Version information.
- **Operating system version** and any Service Packs installed.
- **Installed software packages**, e.g. anti-virus software of other vendors.
- **Exact messages** of the program or of the report file.

11.3 Suspicious file

Viruses that may not yet be detected or removed by our products or suspect files can be sent to us. We provide you with several ways of doing this.

- Identify the file in the Quarantine Manager of the Control Center and select the item Send file via the context menu or the corresponding button.

- Send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus-professional@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

You can also send us the suspect file via our website.

11.4 Reporting false positives

If you believe that Avira AntiVir Professional reports something about a file that is most likely "clean", send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus-professional@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

11.5 Your feedback for more security

At Avira GmbH, the security of our customers is our top priority. For this reason, we don't just have an in-house expert team who tests the quality and security of every Avira GmbH solution before the product is released. We also attach great importance to the indications regarding security relevant gaps which could develop and we treat those frankly.

If you think you have detected a security gap in one of our products, please send us an email to vulnerabilities-professional@avira.com.

12 Reference: Configuration options

The configuration reference documents all configuration options available in Avira AntiVir Professional.

12.1 Scanner

The Scanner section of the Configuration is responsible for the configuration of the on-demand scan.

12.1.1 Scan

Here you define the basic behavior of the scan routine for an on-demand scan. If you select certain directories to be scanned with an on-demand scan, depending on the configuration the Scanner scans:

- with a certain scanning power (priority),
- also boot sectors and main memory,
- certain or all boot sectors and the main memory,
- all or selected files in the directory.

Files

The Scanner can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and file extension. The filter is not used.

Note
If All files is enabled, the button **File extensions** cannot be selected.

Smart Extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by Avira AntiVir Professional. This means that Avira AntiVir Professional decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since not only on the basis of the file extension is scanned. This setting is activated by default and is recommended.

Note
If Smart Extensions is enabled, the button **File extensions** cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button **File extension**.

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the button File extensions.

File extensions

With the aid of this button, a dialog window is opened in which all file extensions are displayed that are scanned in **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the default list may vary from version to version.

Additional settings

Scan boot sectors of selected drives

If this option is enabled, the Scanner only scans the boot sectors of the drives selected for the on-demand scan. This option is enabled as the default setting.

Scan master boot sectors

If this option is enabled, the Scanner scans the master boot sectors of the hard disk(s) used in the system.

Ignore offline files

If this option is enabled, the direct scan ignores so-called offline files completely during a scan. This means that these files are not scanned for viruses and unwanted programs. Offline files are files that were physically moved by a so-called Hierarchical Storage Management System (HSMS) from the hard disk onto a tape, for example. This option is enabled as the default setting.

Integrity checking of system files

When this option is enabled, the most important Windows system files are subjected to a particularly secure check for changes by malware during every on-demand scan. If an amended file is detected, this is reported as suspect. This function uses a lot of computer capacity. That is why the option is disabled as the default setting.

Important
This option is only available with Windows Vista and higher. The option is not available if you are administering Avira AntiVir Professional under SMC.

Note
This option should not be used if you are using third-party tools that modify system files and adapt the boot or start screen to your own requirements. Examples of such tools are skinpacks, TuneUp utilities or Vista Customization.

Optimized scan

When the option is enabled, the processor capacity is optimally utilized during a Scanner scan. For performance reasons, an optimized scan is only logged on standard level.

Note
This option is only available on multi-processor systems. If AntiVir Professional is administered with SMC, the option is always displayed and can be enabled: If the administered system does not have more than one processor, the Scanner option is not used.

Follow symbolic links

If this option is enabled, Scanner performs a scan that follows all symbolic links in the scan profile or selected directory and scans the linked files for viruses and malware. This option is not supported by Windows 2000 and has been deactivated.

Important
The option does not include any shortcuts, but refers exclusively to symbolic links (generated by mklink.exe) or Junction Points (generated by junction.exe) which are transparent in the file system.

Search for Rootkits before scan

If this option is enabled and a scan is started, the scanner scans the Windows system directory for active rootkits in a so-called shortcut. This process does not scan your computer for active rootkits as comprehensively as the scan profile **Scan for rootkits**, but it is significantly quicker to perform.

Important
The rootkit scan is not available for Windows XP 64 bit !

Scan Registry

If this option is enabled, the Registry is scanned for references to malware.

Do not scan files and paths on network drives

If this option is enabled, network drives connected to the computer are excluded from the on-demand scan. This option is recommended when the servers or other workstations themselves are protected with antivirus software , for example other workstation installations of Avira AntiVir Professional. This option is disabled as the default setting.

Scan process

Allow stopping the scanner

If this option is enabled, the scan for viruses or unwanted programs can be terminated at any time with the button Stop in the "Luke Filewalker"window. If you have disabled this setting, the Stop button in the "Luke Filewalker"window has a gray background. Premature ending of a scan process is thus not possible! This option is enabled as the default setting.

Scanner priority

With the on-demand scan, the Scanner distinguishes between priority levels. This is only effective if several processes are running simultaneously on the workstation. The selection affects the scanning speed.

Low

The Scanner is only allocated processor time by the operating system if no other process requires computation time, i.e. as long as only the Scanner is running, the speed is maximum. All in all, work with other programs is optimal: The computer responds more quickly if other programs require computation time while the Scanner continues running in the background. This setting is activated by default and is recommended.

Medium

The Scanner is executed with normal priority. All processes are allocated the same amount of processor time by the operating system. Under certain circumstances, work with other applications may be affected.

High

The Scanner has the highest priority. Simultaneous work with other applications is almost impossible. However, the Scanner completes its scan at maximum speed.

12.1.1.1. Action for concerning files

Action for concerning files

You can define the actions to be carried out by Scanner when a virus or unwanted program is detected.

Interactive

If this option is enabled, the results of the Scanner scan are displayed in a dialog box. When carrying out a scan with the Scanner, you will receive an alert with a list of the affected files at the end of the scan. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the Scanner.

Note
In the Scanner dialog, the action 'Move to quarantine' is displayed as the default action.

Permitted actions

In this display box you can specify those actions that can be selected in the dialog box in the event that a virus is detected in individual or expert notification mode. You must activate the corresponding options for this.

repair

The Scanner repairs the infected file if possible.

rename

The Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. The file can be repaired at a later time and renamed again.

Quarantine

The Scanner moves the file to the Quarantine. The file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center. Depending on the file, further selection options may be available in the Quarantine Manager.

delete

The file will be deleted. This process is much faster than "overwrite and delete".

ignore

The file is to be ignored.

overwrite and delete

The Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Default

The button is used to define a default action by the Scanner to handle the files encountered. Highlight an action and click the **Standard** button. Only the selected default action for the relevant files can be executed in combined notification mode. The selected default action for the relevant files is preselected in individual and expert notification mode.

Note
The action **repair** cannot be selected as the default action.

Note
If you have selected *Delete* or *Overwrite and Delete* as the default action and wish to set the notification mode to combined, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

Click here for more information.

Automatic

If this option is enabled, then no dialog box for selecting an action appears following the detection of a virus or unwanted program. The Scanner reacts according to the settings you define in this section.

Backup to quarantine

If this option is enabled, the Scanner creates a backup copy before carrying out the requested primary or secondary action. The back-up copy is saved in quarantine, where the file can be restored if it is of informative value. You can also send the backup copy to the Avira Malware Research Center for further investigation.

Display detection alerts

If this option is activated, then for each detection of a virus or unwanted program a warning message appears showing the actions being executed.

Primary action

Primary action is the action carried out when the Scanner finds a virus or an unwanted program. If the option **repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.

Note
The option Secondary action can only be selected if the setting **repair** was selected under Primary action.

repair

If this option is enabled, the Scanner repairs affected files automatically. If the Scanner cannot repair an affected file, it carries out the action selected under Secondary action.

Note
An automatic repair is recommended, but means that the Scanner modifies files on the workstation.

delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

overwrite and delete

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Secondary action

The option **Secondary action** can only be selected if the setting **Repair** was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

overwrite and delete

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes (wipes) it. It cannot be restored.

rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Note
If you have selected **Delete**or **Overwrite and Delete** as the primary or secondary action, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

12.1.1.2. Further actions

Launch program following detection

After the on-demand scan, the Scanner can open a file of your choice (for example a program) if at least one virus or unwanted program has been detected, for example an email program, so that you can inform other users or the administrator.

Note
For security reasons it is only possible to start a program after a detection when a user is logged on the computer. The file is then opened with the rights that apply to the logged on user. If no user is logged on, this option is not carried out.

Program name

In this input box you can enter the name and the relevant path of the program that the Scanner should start after a detection.

...

This button opens a window in which you can select the desired program with the aid of the file selection dialog.

Arguments

In this input box you can enter command line parameters for the program to be started if necessary.

Event log

Use event log

If this option is enabled, an event report with the results of the scan is transferred to Windows event logging after a Scanner scan has been completed. The events can be called up in the Windows event viewer. The option is disabled as the default setting.

When scanning archives, the Scanner uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again.

Scan archives

If this option is enabled, the selected archives in the archive list are scanned. This option is enabled as the default setting.

All archive types

If this option is enabled, all archive types in the archive list are selected and scanned.

Smart Extensions

If this option is enabled, the Scanner detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. However, for this every file must be opened - which reduces the scanning speed. Example: if a *.zip archive has the file extension *.xyz, the Scanner also unpacks this archive and scans it. This option is enabled as the default setting.

Note
Only those archive types are supported, which are marked in the archive list.

Limit recursion depth

Unpacking and scanning recursive archives can require a great deal of computer time and resources. If this option is enabled, you limit the depth of the scan in multi-packed archives to a certain number of packing levels (maximum recursion depth). This saves time and computer resources.

Note
In order to find a virus or an unwanted program in an archive, the Scanner must scan up to the recursion level in which the virus or the unwanted program is located.

Maximum recursion depth

In order to enter the maximum recursion depth, the option Limit recursion depth must be enabled.
You can either enter the requested recursion depth directly or by means of the right arrow key on the entry field. The permitted values are 1 to 99. The standard value is 20 which is recommended.

Default values

The button restores the pre-defined values for scanning archives.

Archives

In this display area you can set which archives the Scanner should scan. For this, you must select the relevant entries.

12.1.1.3. Exceptions

File objects to be omitted for the scanner

The list in this window contains files and paths that should not be included by the Scanner in the scan for viruses or unwanted programs.

Please enter as few exceptions as possible here and really only files that, for whatever reason, should not be included in a normal scan. We recommend that you always scan these files for viruses or unwanted programs before they are included in this list!

Note
The entries on the list must not result in more than 6000 characters in total.

Warning
These files are not included in a scan!

Note
The files included in this list are entered in the report file. Please check the report file from time to time for unscanned files, as perhaps the reason you excluded a file here no longer exists. In this case you should remove the name of this file from this list again.

Input box

In this input box you can enter the name of the file object that is not included in the on-demand scan. No file object is entered as the default setting.

The button opens a window in which you can select the required file or the required path.
When you have entered a file name with its complete path, only this file is not scanned for infection. If you have entered a file name without a path, all files with this name (irrespective of the path or drive) are not scanned.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Note
If you add a complete partition to the list of the file objects, only those files which are saved directly under the partition will be excluded from the scan, which does not apply for files in sub-directories on the corresponding partition:
Example: File object to be skipped: `D:\ = D:\file.txt` will be excluded from the scan of the Scanner, `D:\folder\file.txt` will not be excluded from the scan.

12.1.1.4. Heuristic

This configuration section contains the settings for the heuristic of the Avira AntiVir Professional search engine.

Avira AntiVir Professional contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Avira AntiVir Professional contains a highly powerful macro virus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

enable AHeAD

Avira AntiVir Professional contains a very powerful heuristic in the form of AntiVir AheAD technology, which can also detect unknown (new) malware. If this option is activated, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira AntiVir Professional detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This setting is activated by default if you have selected the use of this heuristic.

High detection level

If this option is enabled, Avira AntiVir Professional detects much more unknown malware, however false positives can also be expected.

12.1.2 Report

The Scanner has a comprehensive reporting function. You thus obtain precise information on the results of an on-demand scan. The report file contains all entries of the system as well as alerts and messages of the on-demand scan.

Note
To enable you to establish what actions the Scanner has carried out when viruses or unwanted programs have been detected, a report file should always be created.

Reporting

Off

If this option is enabled, the Scanner does not report the actions and results of the on-demand scan.

Default

When this option is activated, the Scanner logs the names of the files concerned with their path. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

Advanced

When this option is activated, the Scanner logs alerts and tips in addition to the default information.

Complete

When this option is activated, the Scanner also logs all scanned files. In addition, all files involved as well as alerts and tips are included in the report file.

Note
If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

12.2 Guard

The Guard section of the configuration is responsible for the configuration of the on-access scan.

12.2.1 Scan

You will normally want to monitor your system constantly. To this end, use the Guard (= on-access scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

Scan mode

Here the time for scanning of a file is defined.

Scan when reading

If this option is enabled, the Guard scans the files before they are read or executed by the application or the operating system.

Scan when writing

If this option is enabled, the Guard scans a file when writing. You can only access the file again after this process has been completed.

Scan when reading and writing

If this option is enabled, the Guard scans files before opening, reading and executing and after writing. This option is enabled as the default setting and is recommended.

Files

The Guard can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files, irrespective of their content and their file extension, are scanned for viruses or unwanted programs, i.e. the filter is not used.

Note
If All files is enabled, the button File extensions cannot be selected.

Smart Extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by Avira AntiVir Professional. This means that Avira AntiVir Professional decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since not only on the basis of the file extension is scanned.

Note
If Smart Extensions is enabled, the button File extensions cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button File extension. This setting is activated by default and is recommended.

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the button File extensions.

File extensions

With the aid of this button, a dialog window is opened in which all file extensions are displayed that are scanned in **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the file extension list may vary from version to version.

Archives

Scan archives

If this option is enabled, then archives will be scanned. Compressed files are scanned, then decompressed and scanned again. This option is deactivated by default. The archive scan is restricted by the recursion depth, the number of files to be scanned and the archive size. You can set the maximum recursion depth, the number of files to be scanned and the maximum archive size.

Note
This option is deactivated by default, since the process puts heavy demands on the computer's performance. It is generally recommended that archives be checked using an on-demand scan.

Maximum recursion depth

When scanning archives, the Guard uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. You can define the recursion depth. The default value for the recursion depth is 1 and is recommended: all archives that are directly located in the main archive are unpacked and scanned.

Maximum number of files

When scanning archives, you can restrict the scan to a maximum number of files in the archive. The default value for the maximum number of files to be scanned is 10 and is recommended.

Maximum size (KB)

When scanning archives, you can restrict the scan to a maximum archive size to be unpacked. The standard value of 1000KB is recommended.

Drives

Network drives

If this option is enabled, files on network drives (mapped drives) such as server volumes, peer drives etc., are scanned.

Note
In order not to reduce the performance of your computer too much, the option **Network drives** should only be enabled in exceptional cases.

Warning
If this option is disabled, the network drives are **not** monitored. You are no longer protected against viruses or unwanted programs!

Note
When files are executed on network drives, they are scanned by the Guard irrespective of the setting for the *Network Drives* option. In some cases files on network drives are scanned while being opened, even though the *Network Drives* option is disabled. Reason: These files are accessed with 'Execute File' rights. If you want to exclude these files or even executed files on network drives from scanning by the Guard, enter the files in the list of file objects to be excluded (see: Guard::Scan::Exceptions).

Enable caching

If this option is enabled, monitored files on network drives will be made available in the Guard's cache. Monitoring of network drives without the caching function is more secure, but does not perform as well as the monitoring of network drives with caching.

12.2.1.1. Action for concerning files

Action for concerning files

You can define the actions to be carried out by Guard when a virus or unwanted program is detected.

Interactive

If this option is enabled, a desktop notification appears when Guard detects a virus or unwanted program. You have the option of removing the detected malware or accessing other possible virus treatment actions via the 'Details' button. The actions are displayed in a dialog window. Your license data will be displayed in the next window. This option is enabled as the default setting.

Permitted actions

In this display box you can specify the virus management actions that should be available as further actions in the dialog window. You must activate the corresponding options for this.

repair

Guard repairs the infected file if possible.

rename

Guard renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. The file can be repaired at a later time and renamed again.

Quarantine

Guard moves the file to the quarantine folder. The file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center. Depending on the file, further selection options may be available in the Quarantine Manager.

delete

The file will be deleted. This process is much faster than "overwrite and delete".

ignore

Access to the file is permitted and the file is ignored.

overwrite and delete

Guard overwrites the file with a default pattern before deleting it. It cannot be restored.

Deny access

Access is denied to the file. Guard logs the detection to the report file if the report function is activated. In addition, the Guard writes an entry in the Event log, if this option is enabled.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that should be activated by default and click on the **Default** button.

Note
The action **repair** cannot be selected as the default action.

Click here for more information.

Automatic

If this option is enabled, then no dialog box for selecting an action appears following the detection of a virus or unwanted program. Guard reacts according to the settings you define in this section.

Backup to quarantine

If this option is enabled, the Guard creates a backup copy before carrying out the requested primary or secondary action. The backup copy is saved in quarantine. It can be restored via the Quarantine manager if it is of informative value. You can also send the backup copy to the Avira Malware Research Center. Depending on the object, there are more selection possibilities in the Quarantine manager.

Display detection alerts

If this option is enabled, then for each detection of a virus or unwanted program a warning message appears.

Primary action

Primary action is the action carried out when the Guard finds a virus or an unwanted program. If the option **repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.

Note
The option Secondary action can only be selected if the option Repair was selected under Primary action.

repair

If this option is enabled, the Guard repairs affected files automatically. If the Guard cannot repair an affected file, it carries out the action selected under Secondary action.

Note
An automatic repair is recommended, but means that the Guard modifies files on the workstation.

delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

overwrite and delete

If this option is enabled, the Guard overwrites the file with a default pattern and then deletes it. It cannot be restored.

rename

If this option is enabled, the Guard renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Deny access

If this option is enabled, the Guard only enters the detection in the report file if the report function is enabled. In addition, the Guard writes an entry in the Event log, if this option is enabled.

Quarantine

If this option is enabled, the Guard moves the file to the quarantine. The files in this directory can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Secondary action

The option **Secondary action** can only be selected if the option **Repair** was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

overwrite and delete

If this option is enabled, the Guard overwrites the file with a default pattern and then deletes it. It cannot be restored.

rename

If this option is enabled, the Guard renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Deny access

If this option is enabled, the Guard only enters the detection in the report file if the report function is enabled. In addition, the Guard writes an entry in the Event log, if this option is enabled.

Quarantine

If this option is enabled, the Guard moves the file to the quarantine. The files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Note
If you have selected **Delete** or **Overwrite and Delete** as the primary or secondary action, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

12.2.1.2. Further actions

Notifications

Event log

Use event log

When this option is enabled, an entry is added to the event log for every detection. The administrator can identify detections and react accordingly. This option is enabled as the default setting.

Autostart

Block autostart function

When this option is enabled, the execution of the Windows Autostart function is blocked on all connected drives, including USB sticks, CD and DVD drives and network drives. With the Windows Autostart function, files on data media or network drives are read immediately on loading or connection, and files can therefore be started and copied automatically. This functionality however carries with it a high security risk, as malware and unwanted programs can be installed with the automatic start. The Autostart function is especially critical for USB sticks as data on a stick can be changed at any time.

Exclude CDs and DVDs

When this option is enabled, the Autostart function is permitted on CD and DVD drives.

Warning
Only disable the Autostart function for CD and DVD drives if you are sure you are only using trusted data media.

12.2.1.3. Exceptions

With these options you can configure exception objects for the Guard (on-access scan). The relevant objects are then not included in the on-access scan. The Guard can ignore file accesses to these objects during the on-access scan via the list of processes to be omitted. This is useful, for example, with databases or back-up solutions.

Processes to be omitted by the Guard

All file accesses of processes in this list are excluded from monitoring by Guard.

Input box

In this field, enter the name of the process that is to be ignored by the real-time scan. No process is entered as the default setting.

Note
You can enter up to 128 processes.

Note
The entries on the list must not result in more than 6000 characters in total.

Warning:
The specified path and file name of the process should contain a maximum of 255 characters.

Warning
Please note that all file accesses by processes recorded in the list are excluded from the scan for viruses and unwanted programs! The Windows Explorer and the operating system itself cannot be excluded. A corresponding entry in the list is ignored.

The button opens a window in which you can select an executable file.

Processes

The**Processes** button opens the *Process selection* window in which the running processes are displayed.

Add

With this button, you can add the process entered in the input box to the display window.

Delete

With this button you can delete a selected process from the display window.

File objects to be omitted by the Guard

All file accesses to objects in this list are excluded from monitoring by the Guard.

Input box

In this box you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.

Note
The entries in the list must have no more than 6000 characters in total.

Note
For each drive you can specify a maximum of 20 exceptions by entering the complete path (starting with the drive letter).
E.g.: C:\Program Files\Application\Name.log

The maximum number of exceptions without a complete path is 64.
For example: *.log
\computer1\C\directory1

...

The button opens a window in which you can select the file object to be excluded.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

With this button you can delete a selected file object from the display window.

Please observe the following points:

- The file name can only contain the wildcards * (any number of characters) and ? (a single character).
- Directory names must end with a backslash \, otherwise a file name is assumed.
- The list is processed from top to bottom.
- Individual file extensions can also be excluded (inclusive wildcards).
- If a directory is excluded, all its sub-directories are automatically also excluded.
- The longer the list is, the more processor time is required for processing the list for each access. Therefore, keep the list as short as possible.
- In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.
- In order to exclude files and folders on connected network drives from the Guard scan, specify the UNC path you use to connect the network drive in the list of exceptions.
  \\<Computer name>\<Enable>\ - OR - \\<IP address>\<Enable>\

Note
A file name that contains wildcards may not be terminated with a backslash.

For example:

```
C:\Program Files\Application\applic*.exe\
```

This entry is not valid and not treated as an exception!

Note
With regard to exceptions on connected network drives, please note the following: if you use the drive letter of the connected network drive, the files and folders specified are NOT excluded from the Guard scan. If the UNC path in the list of exceptions differs from the UNC path used to connect to the network drive (IP address specification in the list of exceptions – specification of computer name for connection to network drive), the specified folders and files are NOT excluded by the Guard scan. Locate the relevant UNC path in the Guard report file.

Note
In case of dynamic drives which are mounted as a directory on another drive, the alias of the operating system for the integrated drive in the list of the exceptions has to be used: e.g. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
If you use the mount point itself, for example, C:\DynDrive, the dynamic drive will be scanned nonetheless. You can determine the alias of the operating system to be used from the Guard report file.

Note
You can locate the path Guard uses to scan for infected files in the Guard report file. Indicate exactly the same path in the list of exceptions. Proceed as follows: set the protocol function of Guard to **Complete** in the configuration under Guard :: Report. Now access the files, folders, mounted drives or connected network drives with the activated Guard. You can now read the path to be used from the Guard report file. The report file can be accessed in the Control Center under Local protection :: Guard.

Examples:

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Program Files\Application\application.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\applic*
C:\Program Files\Application\applic?????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Application\*.mdb
\\Computer name\Enable\
\\1.0.0.0\Enable\application.exe
```

12.2.1.4. Heuristic

This configuration section contains the settings for the heuristic of the Avira AntiVir Professional search engine.

Avira AntiVir Professional contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Avira AntiVir Professional contains a highly powerful macro virus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

enable AHeAD

Avira AntiVir Professional contains a very powerful heuristic in the form of AntiVir AheAD technology, which can also detect unknown (new) malware. If this option is activated, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira AntiVir Professional detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This setting is activated by default if you have selected the use of this heuristic.

High detection level

If this option is enabled, Avira AntiVir Professional identifies far more unknown malware, but you must also accept that there are likely to be false positives.

12.2.2 ProActiv

AntiVir ProActive protects you from new and unknown threats for which there are not yet any virus definitions or heuristics available. ProActive technology is integrated into the Guard component and observes and analyzes the program actions carried out. The behavior of the program is checked against typical mailware action patterns: Type of action and action sequences. If a program exhibits behavior typical of malware, this is treated as a virus detection : You have the option of blocking the program or ignoring the notification and continuing to use the program. You can classify the program as trusted and add it to the application filter for permitted programs. You have the option of adding the program to the application filter for blocked programs using the *Always block* command.

The ProActive component uses rule sets developed by the Avira Malware Research Center to identify behavior typical of malware. The rule sets are supplied by Avira GmbH databases. AntiVir ProActiv sends information on any suspicious programs detected to the Avira database for logging. You have the option of disabling transmission of data to the Avira databases.

Note
ProActive technology is not yet available for 64 bit systems! Windows 2000 does not support ProActive components.

General

Enabling AntiVir ProActiv.

If this option is enabled, programs are monitored on your computer system and checked for actions typical of malware. You will receive a message if typical malware behavior is detected. You can block the program or select *Ignore* to continue to use the program. The monitoring process excludes: Programs classified as trusted, trusted and signed programs included by default in the permitted applications filter, and all programs which you have added to the application filter for permitted programs.

Be part of the Avira ProActive community

If this option is enabled, AntiVir ProActive sends data on the program actions to the Avira databases. After evaluation, these data are added to the ProActive behavioral analysis rule sets. In this way, you become part of the Avira ProActive community and contribute to the continuous improvement and refinement of the ProActive security technology. No data are sent if this option is disabled. This has no effect on ProActive functionality.

12.2.2.1. Application filter: Applications to be blocked

Under *Application filter: Applications to be blocked* you can enter applications which you classify as harmful and which you want AntiVir ProActive to block by default. The applications added cannot be executed on your computer system. You can also add programs to the application filter for blocking via Guard notifications of suspicious program behavior, by selecting the*Always block this program* option.

Applications to be blocked

Applications

The list contains all applications which you have classified as harmful which you have entered via the configuration or by notifying the ProActive component. The applications on the list are blocked by ProActiv and cannot be executed on your computer system. An operating system message appears when a blocked program starts up. The applications to be blocked are identified by ProActive on the basis of the path specified and the file name, and are blocked irrespective of their content.

Input box

Enter the application you want to block in this box. To identify the application, the full path, file name and file extension must be specified. The path must either include the drive on which the application is located or start with an environment variable.

The button opens a window in which you can select the application to be blocked.

Add

With the **Add** button you can transfer the application specified in the input box to the list of applications to be blocked.

Note
Applications required for the proper operation of the operating system cannot be added.

Delete

The **Delete** button lets you remove a highlighted application from the list of applications to be blocked.

12.2.2.2. Application filter: Permitted applications

The section *Application filter: Permitted applications*lists the applications excluded from monitoring by the ProActiv component: signed programs classified as trusted and included in list by default, all applications classified as trusted and added to the application filter: You can add permitted applications to the list in Configuration. You also have the option of adding applications to suspicious program behavior via Guard notifications by using the **Trusted program** option in the Guard notification.

Applications to be skipped

Applications

The list contains applications excluded from monitoring by the ProActiv component. In the default installation settings, the list contains signed applications from trusted producers. You have the option of adding applications that you consider to be trustworthy via the configuration or via Guard notifications. The ProActive component identifies applications using the path, the file name and the content. We recommend checking the content, as malcode can be added to a program through changes such as updated. You can determine whether a contents check should be carried out from the type specified: For the *Contents* type, the applications specified by path and file name are checked for changes to the file content before they are excluded from monitoring by the ProActiv component. If the file contents have been modified, the application is again monitored by the ProActiv component. For the *Path* type, no contents check is carried out before the application is excluded from monitoring by the Guard. To change the exclusion type, click on the type displayed.

Warning
Only use the *Path* type in exceptional cases. Malcode can be added to an application through an update. The originally harmless application is now malware.

Note
Some trusted applications, including for example all application components of AntiVir Professional, are by default excluded from monitoring by the ProActive component even though they are not included in the list.

Input box

In this box you enter the application to be excluded from monitoring by the ProActiv component. To identify the application, the full path, file name and file extension must be specified. The path must either show the drive on which the application is located or start with an environment variable.

The button opens a window in which you can select the application to be excluded.

Add

With the **Add** button you can transfer the application specified in the input box to the list of applications to be excluded.

Delete

The **Delete** button lets you remove a highlighted application from the list of applications to be excluded.

12.2.3 Report

Guard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Guard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then Guard does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, Guard records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Advanced

If this option is enabled, Guard logs less important information to the report file as well.

Complete

If this option is enabled, Guard logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: 1 to 100 MB. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Backup report file before shortening

If this option is enabled, the report file is backed up before shortening. Save location, see Configuration :: General :: Directories :: Report directory.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

12.3 MailGuard

The MailGuard section of the Configuration is responsible for the configuration of the MailGuard.

12.3.1 Scan

Use MailGuard to scan incoming emails for viruses and malware . Outgoing emails can be scanned for viruses and malware by MailGuard.

Scan

Scan incoming emails

If this option is enabled, incoming emails are scanned for viruses and malware . MailGuard supports POP3 and IMAP protocols. Enable the inbox account used by your email client to receive emails for monitoring by MailGuard.

Monitor POP3 accounts

If this option is enabled, the POP3 accounts are monitored on the specified ports.

Monitored ports

In this field you should enter the port to be used as the inbox by the POP3 protocol. Multiple ports are separated by commas.

Default

This button resets the specified port to the default POP3 port.

Monitor IMAP accounts

If this option is enabled, the IMAP accounts are monitored on the specified ports.

Monitored ports

In this field you should enter the port to be used as the inbox by the IMAP protocol. Multiple ports are separated by commas.

Default

This button resets the specified port to the default IMAP port.

Scan outgoing emails (SMTP)

If this option is enabled, outgoing emails are scanned for viruses and malware.

Monitored ports

In this field you should enter the port to be used as the outbox by the SMTP protocol. Multiple ports are separated by commas.

Default

This button resets the specified port to the default SMTP port.

Note
To verify the protocols and ports used, call up the properties of your email accounts in your email client program. Default ports are mostly used.

12.3.1.1. Action for concerning files

This configuration section contains settings for actions performed when MailGuard finds a virus or unwanted program in an email or in an attachment.

Note
These actions are performed both when a virus is detected in incoming emails and when a virus is detected in outgoing emails.

Action for concerning files

Interactive

If this option is enabled, a dialog window appears when a virus or unwanted program is detected in an email or attachment in which you can choose what is to be done with the email or attachment concerned. This option is enabled as the default setting.

Permitted actions

In this display box you can specify those actions that are to be displayed in the dialog box in the event that a virus or unwanted program is detected. You need to activate the corresponding options.

Move to quarantine

When this option has been activated, the email including all attachments is moved to quarantine. It can be mailed by the quarantine manager later. The affected email is deleted. The body of the text and any attachments of the email are replaced by a standard text.

Delete

If this option is enabled, the affected email is deleted when a virus or unwanted program is detected. The body of the text and any attachments of the email are replaced by a standard text.

Delete attachment

If this option has been activated, the attachment concerned is replaced by a standard text. If the body of the text of the email is affected, it will be erased and also replaced by a standard text. The email itself is delivered.

Move attachment to quarantine

If this option has been activated, the attachment affected is moved to quarantine and subsequently erased (replaced by a standard text). The body of the email is delivered. The affected attachment can be delivered later by the quarantine manager.

Ignore

If this option is enabled, an affected email is delivered despite detection of a virus or unwanted program.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that should be activated by default and click on the **Default** button.

Show progress bar

If this option is enabled, the MailGuard shows a progress bar during downloading of emails. This option can only be enabled if the option **Interactive** has been selected.

Automatic

If this option is enabled, you are no longer notified when a virus or unwanted program is found. MailGuard reacts according to the settings you define in this section.

Primary action

Primary action is the action carried out when the MailGuard finds a virus or an unwanted program in an email. If the option **Ignore email** is selected, it is also possible to select under **Affected attachments** what is to be done if a virus or unwanted program is detected in an attachment.

delete email

If this option is enabled, the affected email is automatically deleted if a virus or unwanted program is found. The body of the email is replaced by the default text given below. The same applies to all attachments included; these are also replaced by a default text.

Isolate email

If this option is enabled, the complete email including all attachments is placed in Quarantine if a virus or unwanted program is found. If required, it can later be restored. The affected email itself is deleted. The body of the email is replaced by the default text given below. The same applies to all attachments included; these are also replaced by a default text.

ignore email

If this option is enabled, the affected email is ignored despite detection of a virus or unwanted program. However, you can decide what is to be done with the affected attachment:

Affected attachments

The option **Affected attachments** can only be selected if the setting **Ignore email** has been selected under **Primary action**. With this option it is now possible to decide what is to be done if a virus or unwanted program is found in an attachment.

delete

If this option is enabled, the affected attachment is deleted if a virus or unwanted program is found and replaced by a default text.

isolate

If this option is enabled, the affected attachment is placed in quarantine and then deleted (replaced by a default text). If required, it can later be restored.

ignore

If this option is enabled, the attachment is ignored despite detection of a virus or unwanted program and delivered.

Warning
If you select this option, you have no protection against viruses and unwanted programs by the MailGuard. Only select this item if you are certain you know what you are doing. Disable the preview in your email program, never open attachments by double-clicking!

12.3.1.2. Other Actions

This configuration section contains other settings for actions performed when MailGuard finds a virus or unwanted program in an email or in an attachment.

Note
These actions are performed exclusively when a virus is detected in incoming emails.

Default text for deleted and moved emails

The text in this box is inserted in the email as a message instead of the affected email. You can edit this message. You can enter a maximum of 500 characters.

You can use the following key combination for formatting:

Strg + Enter inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

Default text for deleted and moved attachments

The text in this box is inserted in the email as a message instead of the affected attachment. You can edit this message. You can enter a maximum of 500 characters.

You can use the following key combination for formatting:

Strg + Enter inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

12.3.1.3. Heuristic

This configuration section contains the settings for the heuristic of the Avira AntiVir Professional search engine.

Avira AntiVir Professional contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristic

Activate macrovirus heuristics

Avira AntiVir Professional contains a highly powerful macro virus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

enable AHeAD

Avira AntiVir Professional contains a very powerful heuristic in the form of AntiVir AheAD technology, which can also detect unknown (new) malware. If this option is activated, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira AntiVir Professional detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This option is enabled as the default setting if you have selected application of this heuristic. This option is enabled as the default setting and is recommended.

High detection level

If this option is enabled, Avira AntiVir Professional detects much more unknown malware, however false positives can also be expected.

12.3.2 General

12.3.2.1. Exceptions

Email addresses not scanned

This table shows you the list of email addresses excluded from scanning by AntiVir MailGuard (white list).

Note
The list of exceptions is used exclusively by MailGuard with regard to incoming emails.

Status

Icon	Description
	This email address will no longer be scanned for malware.

Email address

Email that is no longer to be scanned.

Malware

When this option is enabled, the email address is no longer scanned for malware.

Up

You can use this button to move a highlighted email address to a higher position. If no entry is highlighted or the highlighted address is at the first position in the list, this button is not enabled.

Down

You can use this button to move a highlighted email address to a lower position. If no entry is highlighted or the highlighted address is at the last position in the list, this button is not enabled.

Input box

In this box you enter the email address that you want to add to the list of email addresses not to be scanned. Depending on your settings, the email address will no longer be scanned in future by the MailGuard.

Add

With this button you can add the email address entered in the input box to the list of email addresses not to be scanned.

Delete

This button deletes a highlighted email address from the list.

12.3.2.2. Cache

Cache

The MailGuard cache contains data regarding the scanned emails that is displayed as statistical data in the Control Center under MailGuard.

Maximum number of emails to be stored in the cache

This field is used to set the maximum number of emails that are stored by MailGuard in the cache. Emails are deleted oldest first.

Maximum storage period of an email in days

The maximum storage period of an email in days is entered in this box. After this time, the email is removed from the cache.

Empty Cache

Click on this button to delete the emails stored in the cache.

12.3.2.3. Footer

Under *Footer* you can configure an email footer which is displayed in the emails you send. This function requires activation of the MailGuard scan of outgoing emails (see option *Scan outgoing emails (SMTP)* under Configuration::MailGuard::Scan) . You can use the defined AntiVir MailGuard footer to confirm the sent email has been scanned by a virus protection program. You also have the option of inserting text yourself for a user-defined footer. If you use both footer options, the user-defined text is preceded by the AntiVir MailGuard footer.

Footer for emails to be sent

Attach AntiVir MailGuard footer

If this option is enabled, the AntiVir MailGuard footer is displayed beneath the message text of the sent email. The AntiVir MailGuard footer confirms that the sent email has been scanned for viruses and unwanted programs by AntiVir MailGuard. The AntiVir MailGuard footer contains the following text: "Scanned with AntiVir MailGuard [product version] [initials and version number of search engine] [initials and version number of virus definition file]".

Attach this footer

If this option is enabled, the text which you insert into the input box is displayed as a footer in sent emails.

Input box

If this option is enabled, the text which you insert into the input box is displayed as a footer in sent emails.

12.3.3 Report

MailGuard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then MailGuard does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, MailGuard records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Advanced

If this option is enabled, MailGuard logs less important information to the report file as well.

Complete

If this option is enabled, MailGuard logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Backup report file before shortening

If this option is enabled, the report file is backed up before shortening. Save location, see Configuration :: General :: Directories :: Report directory.

Write configuration in report file

If this option is enabled, the MailGuard configuration is recorded in the report file.

12.4 Firewall

The Firewall section of Configuration is responsible for configuration of the Avira Firewall.

12.4.1 Adapter rules

In the Avira Firewall, an adapter represents a software simulated hardware device (e.g. miniport, bridge connection, etc.) or a real hardware device (e.g. network card).

The Avira Firewall displays the adapter rules of all existing adapters on your computer for which a driver was installed.

A predefined adapter rule depends on the security level. You can change the security level in the Online protection::Firewall section of the Avira AntiVir Professional Control Center or you can define your own adapter rules. If you have defined your own adapter rules, in the Firewall section of the Avira AntiVir Professional Control Center, the security level is set to custom.

Note
The defaultsecurity level setting for all predefined rules of the Avira Firewall is **High**

ICMP protocol

The Internet Control Message Protocol (ICMP) is used to exchange error and information messages on networks. The protocol is also used for status messages with ping or tracer.
With this rule you can define the incoming and outgoing blocked message types, the behavior in case of flooding and the reaction of fragmented ICMP packets. This rule serves for preventing so-called ICMP flood attacks, which results in an increase of the CPU load of the attacked machine as it responds to every packet.

Predefined rules for the ICMP protocol

Setting: Low	**Setting: Medium**	**Setting: High**
Incoming blocked types: **no type**. Outgoing blocked types: **no type**. Assume flooding if delay between packets is less than **50** ms. **Reject** fragmented ICMP packets.	Same rule as for the low level.	Incoming blocked types: **several types** Outgoing blocked types: **several types** Assume flooding if delay between packets is less than **50** ms. **Reject** fragmented ICMP packets.

Incoming blocked type: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can specify the desired incoming ICMP message types you want to block.

Outgoing blocked type: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can select the desired outgoing ICMP message types you want to block.

Flooding

With a mouse click on the link a dialog box is displayed where you can enter the maximum allowed ICMPA delay.

Fragmented ICPM packets

With a mouse click on the link you have the choice to reject or not to reject fragmented ICMP packets.

TCP port scan

With this rule you can define when a TCP port scan is assumed by the Firewall and what should be done in this case. This rule serves for preventing so-called TCP port scan attack, which results in a detection of open TCP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the TCP port scan

Setting: Low	Setting: Medium	Setting: High
Assume a TCP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **don't add** rule to block the attack.	Assume a TCP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.	Same rule as for medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a TCP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a TCP port scan is assumed.

Report file

With a mouse click on the link you have the choice to log or don't log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or not to add the rule to block the TCP port scan attack.

UDP port scan

With this rule you can define when a UDP port scan is assumed by the Firewall and what should be done in this case. This rule prevents so-called UDP port scan attacks, which result in a detection of open UDP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the UDP port scan

Setting: Low	Setting: Medium	Setting: High
Assume a UDP port scan if **50** or more ports were scanned in **5,000**	Assume a UDP port scan if **50** or more ports were scanned in **5,000**	Same rule as for medium level.

milliseconds. When detected,**log** attacker's IP and **don't add** rule to block the attack.	milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.	

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a UDP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a UDP port scan is assumed.

Report file

With a mouse click on the link you have the choice to log or don't log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or not to add the rule to block the UDP port scan attack.

12.4.1.1. Incoming Rules

Incoming rules are defined to control incoming traffic by the Avira Firewall.

Note
When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Predefined rules for the TCP traffic monitor

Setting: Low	**Setting: Medium**	**Setting: High**
No incoming traffic is blocked by the Avira Firewall.	– Allow Established TCP Connections on 135 **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{135}** and remote ports in **{0-65535}**. Apply for**packets of existing connections**. **Don't log** when packet matches rule. Advanced:	– Monitor established TCP traffic **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{0-65535}** and remote ports in **{0-65535}**. Apply for**packets of existing connections**. **Don't log** when packet matches rule.

	Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Deny TCP packets on 135 Deny **TCP packets** from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{135}** and remote ports in **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Monitor TCP healthy traffic **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{0-65535}** and remote ports in **{0-65535}**. Apply for **connection initiation and existing connection packets.** **Don't log** when packet matches	Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

	rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Deny all TCP packets Deny **TCP packets**from address **0.0.0.0** with mask **0.0.0.0** if local ports are in range **{0-65535}** and the remote port is in range **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	

Accept / deny TCP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming TCP packets.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply the rule for connection initiation and existing connection packets or only for packets of existing connections or for all packets.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where TCP header ends.

Predefined rules for the UDP traffic monitor

Setting: Low	Setting: Medium	Setting: High
-	– Monitor UDP accepted traffic **Allow** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0- 66535}** and remote port is in **{0-66535}**. Apply rule to **open ports**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	Monitor established UDP traffic monitor Allow **UDP packets** from address **0.0.0.0** with mask **0.0.0.0** if the local port is in range **{0-65535}** and the remote port is in range **{53, 67, 68, 123}**. Apply rule to **open ports**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

	– Deny all UDP packets Deny **UDP packets** from address **0.0.0.0** with mask **0.0.0.0**if the local port is in range **{0-65535}** and the remote port is in range **{0-65535}**. Apply for **all ports**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	

Accepting of UDP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming UDP packets.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply this rule to all ports or only to all opened ports.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where UDP header ends.

Predefined rules for the ICMP traffic monitor

Setting: Low	Setting: Medium	Setting: High
-	– Do not discard ICMP based on IP address **Allow** ICMP packets from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	Same rule as for medium level.

Accepting of ICMP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming ICMP packets.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where ICMP header ends.

Predefined rules for IP packets

Setting: Low	Setting: Medium	Setting: High
-	-	Deny all IP packets Deny **IP packets** from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule.

Accepting/rejecting IP packets

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

Possible rules for monitoring IP packages based on IP protocols

IP packages

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Protocol

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP protocol.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

12.4.1.2. Outgoing Rules

Outgoing rules are defined to control outgoing traffic by the Avira Firewall. You can define an outgoing rule for one of the following protocols: IP, ICMP, UDP and TCP.

Note
When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Buttons

Button	Description
Add	Allows you to create a new rule. If you press this button, the "Add new rule" dialog box is opened. In this dialog box you can select new rules.
Remove	Removes the selected rule.
Rule down	Moves the selected rule down one line, i.e. reduces the rule priority.
Rule up	Moves the selected rule up one line, i.e. increases the rule priority.
Rename	Allows you to give the selected rule another name.

Note
You can add new rules for individual adapters or for all adapters present on the computer. To add an adapter rule for all adapters, select **Computer** from the adapter hierarchy that is displayed and click on the **Add** button.

Note
To change the position of a rule you can also use the mouse to drag the rule to the required position.

12.4.2 Application rules

Application rules for user

This list contains all users in the system. If you are logged in as an administrator, you can select the user you want to apply the rules for. If you are not a privileged user, you can see only the user currently logged on.

Application list

This table shows the list of applications for which rules are defined. The application list contains the settings of each application that was executed and had a rule saved since the Avira Firewall was installed.

Normal view

	Description
Application	Name of the application.
Mode	Displays the selected application rule mode : In **filtered** mode, adapter rules are checked and executed after execution of the application rule. In *privileged* mode, adapter rules are ignored. Click on the link to switch to a different mode.
Action	Shows the action that the Avira Firewall will automatically take when the application is using the network, whatever the network usage type is. With a mouse click on the link you can switch to another action type. The action types are **Ask**, **Allow** or **Deny**. **Ask** is the default action.

Extended configuration

If the network accesses of an application require individual rules, you can create the application rules based on packet filters in the same way as you created the adapter rules. To change to the extended configuration of the application rules, first activate expert mode. Then change the applications rules setting in the Firewall::Settings section: Enable the **Extended Settings** option and save the setting by clicking **Accept** or **OK**. In the firewall configuration, select the **Firewall::Application rules** section: An additional column with the heading *Filtering* with the entry *Simple* is displayed in the list of application rules. You now have an additional **Filtering:** *Advanced - Action: rules* option, which enables you to select the extended configuration.

	Description
Application	Name of the application.
Mode	Displays the selected application rule mode : In **filtered** mode, adapter rules are checked and executed after execution of the application rule. In *privileged* mode, adapter rules are ignored. Click on the link to switch to a different mode.
Action	Shows the action that the Avira Firewall will automatically take when the application is using the network, whatever the network usage type is. If you choose *Filtering - Simple*, you can click the link to select another action type. The action types are **Ask**, **Allow, Deny** or *Extended*. If you choose *Filtering - Advanced*, the *Rules* action type is displayed. The **Rules** link opens the **Application rules** window,

	in which you can enter specific rules for the application.
Filtering	Shows the type of filtering. You can select another type of filtering by clicking the link. *Simple*: In the case of simple filtering, the specified action is carried out on all network activities performed by the software application. *Advanced*: With this type of filtering, the rules that were added to the extended configuration are applied.

If you want to create specific rules for an application, select the **Advanced** entry under *Filtering*. The *Rules* entry is then displayed in the **Action** column. Click on **Rules** to open the window for creating specific application rules.

Specified application rules in the extended configuration

Specified application rules allow you to allow or deny specified data traffic for the application or allow or deny passive listening to individual ports. The following options are available:

- Allow or deny code injection

  Code injection is a technique for introducing code into the address space of another process to execute actions, forcing this process to load a dynamic link library (DLL). Code injection is used by malware, amongst other things, to execute code under cover of another program. In this way, access to the Internet in front of the Firewall can be hidden. In default mode, code injection is enabled for all signed applications.

- Allow or deny passive listening to the application of ports
- Allow or deny data traffic

Allow or deny incoming and/or outgoing IP packets

Allow or deny incoming and/or outgoing TCP packets

Allow or deny incoming and/or outgoing UDP packets

You can create as many application rules as you like for each application. The application rules are executed in the sequence shown .

Note
If you change the *Advanced* filtering of an application rule, the already existing application rules in the extended configuration are simply deactivated, not irretrievably deleted. If you select *Advanced* filtering again, the already existing application rules will be reactivated and displayed in the extended configuration for application rules window.

Application details

In this box you can see details of the application selected in the application list box.

	Description
Name	Name of the application.
Path	Full path to the executable file.

Buttons

Button	Description
Add application	Allows you to create a new application rule. If you press this button, a dialog window is opened. Here you can select the required application for creating a new rule.
Remove rule	Removes the selected application rule.
Reload	Reloads the list of applications and simultaneously discards the changes just made to the application rules.

12.4.3 Trusted vendors

A list of trusted software producers is displayed under *Trusted providers*. You can add / remove producers to / from the list using the *Always trust this provider* option in the *Network Event* popup window. You can allow network access from applications that are signed by the listed providers by default, by enabling the **Automatically allow applications from trusted providers** option.

Trusted vendors for user

This list contains all users in the system. If you are logged in as an administrator, you can select the user whose list of trusted providers you want to view or update. If you are not a privileged user, you can see only the user currently logged on.

Automatically allow applications created by trusted vendors

If this option is enabled, the application provided with the signature of a known and trusted provider is automatically permitted access to the network. The option is enabled as the default setting.

Vendors

The list shows all providers classified as trusted.

Buttons

Button	Description
Remove	The highlighted entry is removed from the list of trusted providers. To permanently remove the selected provider from the list, click **Accept** or **OK** in the configuration window.
Reload	The changes made are reversed. The last list saved is loaded.

Note
If you remove providers from the list and then select **Apply** the providers will be permanently removed from the list. The change cannot be reversed with *Reload*. However, you can use the *Always trust this provider* option in the *Network Event* popup window to add a provider to the list of trusted providers again.

Note
The Firewall prioritizes application rules before making entries in the list of trusted providers: If you have created an application rule and the application provider is listed in the list of trusted providers, the application rule will be executed.

12.4.4 Settings

Advanced options

Firewall enable

If the option is activated, the Avira Firewall is enabled and protects your computer from risks originating from the Internet and other networks.

Stop Windows Firewall on startup

If this option is enabled, the Windows Firewall is deactivated when the computer is rebooted. This option is enabled as the default setting.

Windows Host file is not locked/locked.

If this option is set to LOCKED, the windows host file is write protected. Manipulation is no longer possible. For example, malware is not able to redirect you to undesired websites. The state of this option is NOT LOCKED as the default setting.

Automatic rule timeout

Block forever

If this option is enabled, a rule that was automatically created, for example, during a port scan is retained.

Remove rule after n seconds

If this option is enabled, a rule that was automatically created for example during a port scan, is removed again after the time you have defined. This option is enabled as the default setting.

Notifications

Notifications define the events under which you wish to receive a desktop notification from the Firewall.

Port scan

If the option is activated, you will receive a desktop notification if a port scan has been detected by the Firewall.

Flooding

If the option is activated, you will receive a desktop notification if a flooding attack has been detected by the Firewall.

Applications blocked

If the option is activated, you will receive a desktop notification if the Firewall has denied, i.e. blocked, network activity by an application.

IP blocked

If the option is activated, you will receive a desktop notification if the Firewall has denied, i.e. blocked, data traffic from an IP address.

Application rules

The application rules options are used to set the configuration options for application rules in the Firewall::Application rules section.

Advanced options

If this option is enabled, you can regulate different network accesses of an application on an individual basis.

Basic settings

If this option is enabled, only one action can be set for different network accesses of the application.

Preferred mode

Users who are not administrators can change authorizations for applications

If the option is enabled, all users can change application rules or create new ones. If this option is disabled, only users with administrator rights can change application rules or create new ones. Application rules are displayed in the configuration under Firewall::Application rules, where they can be changed or added. Application rules can be chnaged in the Control Center under Online protection::Firewall and in the Network event window.

12.4.5 Popup settings

Popup settings

Inspect process launch stack

If this option is enabled, the process stack inspection allows a more accurate control. The Firewall will assume that any of the untrustworthy processes in the stack may actually be the one accessing the network through its child process. Therefore a different popup window will be opened for each untrustworthy process in the process stack. This option is disabled as the default setting.

Allow multiple popups per process

If this option is enabled, every time an application is making a network connection, a popup is triggered. Alternatively you will be informed only on the first connection attempt. This option is disabled as the default setting.

Automatically disable popup notification in gaming mode

When this option is active, Avira Firewall gaming mode is automatically activated when an application is executed in full-screen mode on your computer system. In gaming mode, all defined adapter and application rules apply. Applications for which no rules are defined with the *Allow* or *Deny* actions are temporarily allowed to access the network, so that no popup windows appear with questions about the network event.

Remember the action for this application

Always enabled

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is activated as the default setting. This option is enabled as the default setting.

Always disabled

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is disabled as the default setting.

Allow signed application

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is automatically enabled during network access by signed applications. The manufacturers are: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Remember last used state

When this option is enabled, the option "Save action for this application" in the dialog box "Network event" is enabled in the same way as for the last network event. If the option "Save action for this application" of the dialog box "Network event" was enabled, this option is enabled for the following network event. If the option "Save action for this application" was disabled for the last network event, this option is also disabled for the following network event.

Show details

In this group of configuration options, you can setup the display of detailed information in the **Network event** window.

Show details on demand

If this option is enabled, the detailed information is only displayed in the*Network event* window on request, i.e. the detailed information is displayed by clicking on the **Show details** button in the *Network event* window.

Always show details

If this option is enabled, detailed information is always displayed in the *Network event* window.

Remember last used state

If this option is enabled, the display of detailed information is administered in the same way as for the previous network event. If detailed information was displayed or accessed during the last network event, detailed information is displayed for the following network event. If detailed information was hidden and not displayed during the last network event, detailed information is not displayed for the following network event.

Allow privileged

In this group of configuration options, you can define the status of the *Allow privileged* option in the **Network event** window.

Always enabled

If this option is enabled, the *Allow privileged* option is enabled as the default setting in the *Network event* window.

Always disabled

If this option is enabled, the *Allow privileged* option is disabled as the default setting in the *Network event* window.

Remember last used state

If this option is enabled, the status of the *Allow privileged* option is handled in the same way as for the previous network event in the *Network event* window: If the option *Allow privileged* was enabled for execution of the last network event, the option is enabled by default for the following network event. If the option *Allow privileged* was disabled for execution of the last network event, the option is disabled by default for the following network event.

12.5 Firewall under SMC

The firewall of AntiVir Professional is configured to meet the specific requirements of an administration through the Avira Security Management Center. Extended options and restrictions exist for individual configuration options:

- The firewall settings apply to all users of the client computer
- Adapter rules: Security levels for individual adapters can be set using context menus
- Application rule: Network access by applications can be allowed or denied. There is no way of creating specific application rules.

If Avira AntiVir Professional is administered by the Avira Security Management Center, the following firewall setting options in the AntiVir Professional Control Center on client computers are deactivated:

- Setting of the firewall safety levels
- Setting of adapter and application rules

12.5.1 General settings

Advanced options

Lock Windows host file

If the option is enabled, the Windows host file is write protected. Manipulation is no longer possible. For example, malware is not able to redirect you to undesired websites.

Game Mode enable

When this option is active, Avira Firewall gaming mode is automatically activated when an application is executed in full-screen mode on your computer system. In gaming mode, all defined adapter and application rules apply. Applications for which no rules are defined with the *Allow* or *Deny* actions are temporarily allowed to access the network, so that no popup windows appear with questions about the network event.

Stop Windows Firewall on startup

If this option is enabled, the Windows Firewall is deactivated when the computer is rebooted. This option is enabled as the default setting.

Firewall enable

If the option is activated, the Avira Firewall is enabled and protects your computer from risks originating from the Internet and other networks.

Automatic rule timeout

Block forever

If this option is enabled, a rule that was automatically created, for example, during a port scan is retained.

Remove rule after n seconds

If this option is enabled, a rule that was automatically created for example during a port scan, is removed again after the time you have defined. This option is enabled as the default setting.

12.5.2 General adapter rules

Network connections that have been set up are designated adapters. Adapter rules can be drawn up for the following Client network connections:

- Default adapter: LAN or high-speed internet
- Wireless
- Dial-up connection

Form the adapter's context menu you can specify pre-defined adapter rules for every available adapter:

- Security level - High
- Security level - Medium
- Security level - Low

You also have the option of modifying individual adapter rules to suit your own particular requirements.

Note
The default security level setting for all predefined rules of the Avira Firewall is **High**

ICMP protocol

The Internet Control Message Protocol (ICMP) is used to exchange error and information messages on networks. The protocol is also used for status messages with ping or tracer.
With this rule you can define the incoming and outgoing blocked message types, the behavior in case of flooding and the reaction of fragmented ICMP packets. This rule serves for preventing so-called ICMP flood attacks, which results in an increase of the CPU load of the attacked machine as it responds to every packet.

Predefined rules for the ICMP protocol

Setting: Low	**Setting: Medium**	**Setting: High**
Incoming blocked types: **no type**. Outgoing blocked types: **no type**. Assume flooding if delay between packets is less than	Same rule as for the low level.	Incoming blocked types: **several types** Outgoing blocked types: **several types** Assume flooding if delay between packets is less than

50 ms. **Reject** fragmented ICMP packets.		**50** ms. **Reject** fragmented ICMP packets.

Incoming blocked type: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can specify the desired incoming ICMP message types you want to block.

Outgoing blocked type: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can select the desired outgoing ICMP message types you want to block.

Flooding

With a mouse click on the link a dialog box is displayed where you can enter the maximum allowed ICMPA delay.

Fragmented ICPM packets

With a mouse click on the link you have the choice to reject or not to reject fragmented ICMP packets.

TCP port scan

With this rule you can define when a TCP port scan is assumed by the Firewall and what should be done in this case. This rule serves for preventing so-called TCP port scan attack, which results in a detection of open TCP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the TCP port scan

Setting: Low	Setting: Medium	Setting: High
Assume a TCP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **don't add** rule to block the attack.	Assume a TCP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.	Same rule as for medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a TCP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a TCP port scan is assumed.

Report file

With a mouse click on the link you have the choice to log or don't log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or not to add the rule to block the TCP port scan attack.

UDP port scan

With this rule you can define when a UDP port scan is assumed by the Firewall and what should be done in this case. This rule prevents so-called UDP port scan attacks, which result in a detection of open UDP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the UDP port scan

Setting: Low	Setting: Medium	Setting: High
Assume a UDP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected,**log** attacker's IP and **don't add** rule to block the attack.	Assume a UDP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.	Same rule as for medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a UDP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a UDP port scan is assumed.

Report file

With a mouse click on the link you have the choice to log or don't log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or not to add the rule to block the UDP port scan attack.

12.5.2.1. Incoming Rules

Incoming rules are defined to control incoming traffic by the Avira Firewall.

Note
When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Predefined rules for the TCP traffic monitor

Setting: Low	Setting: Medium	Setting: High
No incoming traffic is blocked by the Avira Firewall.	– Allow Established TCP Connections on 135	– Monitor established TCP traffic

	Allow TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{135}** and remote ports in **{0-65535}**. Apply for**packets of existing connections**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Deny TCP packets on 135 Deny **TCP packets** from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{135}** and remote ports in **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Monitor TCP healthy traffic **Allow** TCP	**Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{0-65535}** and remote ports in **{0-65535}**. Apply for**packets of existing connections**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

	packets from address **0.0.0.0** with mask **0.0.0.0** if local ports in **{0-65535}** and remote ports in **{0-65535}**. Apply for **connection initiation and existing connection packets.** **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Deny all TCP packets Deny **TCP packets**from address **0.0.0.0** with mask **0.0.0.0** if local ports are in range **{0-65535}** and the remote port is in range **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	

Accept / deny TCP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming TCP packets.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply the rule for connection initiation and existing connection packets or only for packets of existing connections or for all packets.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where TCP header ends.

Predefined rules for the UDP traffic monitor

Setting: Low	Setting: Medium	Setting: High
-	– Monitor UDP accepted traffic **Allow** UDP packets from address **0.0.0.0** with mask **0.0.0.0**	Monitor established UDP traffic monitor Allow **UDP packets** from address **0.0.0.0** with mask **0.0.0.0** if

	if local port is in **{0- 66535}** and remote port is in **{0-66535}**. Apply rule to **open ports**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. – Deny all UDP packets Deny **UDP packets** from address **0.0.0.0** with mask **0.0.0.0**if the local port is in range **{0-65535}** and the remote port is in range **{0-65535}**. Apply for **all ports**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	the local port is in range **{0-65535}** and the remote port is in range **{53, 67, 68, 123}**. Apply rule to **open ports**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

Accepting of UDP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming UDP packets.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply this rule to all ports or only to all opened ports.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where UDP header ends.

Predefined rules for the ICMP traffic monitor

Setting: Low	Setting: Medium	Setting: High
-	– Do not discard ICMP based on IP address **Allow** ICMP packets from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.	Same rule as for medium level.

Accepting of ICMP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming ICMP packets.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where ICMP header ends.

Predefined rules for IP packets

Setting: Low	Setting: Medium	Setting: High
-	-	Deny all IP packets Deny **IP packets** from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule.

Accepting/rejecting IP packets

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

Possible rules for monitoring IP packages based on IP protocols

IP packages

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Protocol

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP protocol.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

12.5.2.2. Outgoing Rules

Outgoing rules are defined to control outgoing traffic by the Avira Firewall. You can define an outgoing rule for one of the following protocols: IP, ICMP, UDP and TCP.

Note
When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Buttons

Button	Description
Add	Allows you to create a new rule. If you press this button, the "Add new rule" dialog box is opened. In this dialog box you can select new rules.
Remove	Removes the selected rule.
Rule down	Moves the selected rule down one line, i.e. reduces the rule priority.
Rule up	Moves the selected rule up one line, i.e. increases the rule priority.
Rename	Allows you to give the selected rule another name.

Note
You can add new rules for individual adapters or for all adapters present on the computer. To add an adapter rule for all adapters, select **Computer** from the adapter hierarchy that is displayed and click on the **Add** button.

Note
To change the position of a rule you can also use the mouse to drag the rule to the required position.

12.5.3 Application list

You can use the application list to create rules specifying how applications access networks. You can add applications to lists and set the *Allow* and **Block** rules for the selected application using a context menu:

- Access to networks by applications with the *Allow* rule is permitted.
- Access to networks by applications with the *Block* rule is denied.

When applications are added, the *Allow* rule is set. All applications that are added are uniquely identified using the MD5 checksum. If an application changes following an update, for example, the application with the rule in question is automatically removed from the application list. Following a change, the application must be added to the list again and the desired rule reapplied.

Application list

This table shows the list of applications for which rules are defined. The symbols indicate whether network access by the applications is allowed or denied. The rules for the applications can be changed using a context menu.

Buttons

Button	Description
Add	This button opens a dialog box in which you can select applications. The application is added to the application list with the rule 'Allow network access'.
Add group	This button opens a dialog box in which you can select a directory. All applications in the selected path are added to the application list with the rule 'Allow network access'.
Remove	The selected application rule is removed.
Remove all	All application rules are removed.

12.5.4 Trusted vendors

A list of trusted software producers is displayed under *Trusted providers*. Applications from the listed software manufacturers will be granted access to the network. You can add and remove manufacturers from the list.

Vendors

The list shows all providers classified as trusted.

Buttons

Button	Description
Add	This button opens a dialog box in which you can select applications. The manufacturer of the application is established and added to the list of trusted providers.
Add group	This button opens a dialog box in which you can select a directory. The manufacturers of all the applications in the selected path are established and added to the list of trusted providers.
Remove	The highlighted entry is removed from the list of trusted providers. To permanently remove the selected provider from the list, click **Accept** or **OK** in the configuration window.
Remove all	All entries are removed from the list of trusted providers.
Reload	The changes made are reversed. The last list saved is loaded.

Note
If you remove providers from the list and then select **Apply** the providers will be permanently removed from the list. The change cannot be reversed with *Reload*.

Note
The Firewall prioritizes application rules before making entries in the list of trusted providers: If you have created an application rule and the application provider is listed in the list of trusted providers, the application rule will be executed.

12.5.5 Additional settings

Notifications

Notifications define the events under which you wish to receive a desktop notification from the Firewall.

Port scan

If the option is activated, you will receive a desktop notification if a port scan has been detected by the Firewall.

Flooding

If the option is activated, you will receive a desktop notification if a flooding attack has been detected by the Firewall.

Applications blocked

If the option is activated, you will receive a desktop notification if the Firewall has denied, i.e. blocked, network activity by an application.

IP blocked

If the option is activated, you will receive a desktop notification if the Firewall has denied, i.e. blocked, data traffic from an IP address.

Popup settings

Inspect process launch stack

If this option is enabled, the process stack inspection allows a more accurate control. The Firewall will assume that any of the untrustworthy processes in the stack may actually be the one accessing the network through its child process. Therefore a different popup window will be opened for each untrustworthy process in the process stack. This option is disabled as the default setting.

Allow multiple popups per process

If this option is enabled, every time an application is making a network connection, a popup is triggered. Alternatively you will be informed only on the first connection attempt. This option is disabled as the default setting.

Automatically disable popup notification in gaming mode

When this option is active, Avira Firewall gaming mode is automatically activated when an application is executed in full-screen mode on your computer system. In gaming mode, all defined adapter and application rules apply. Applications for which no rules are defined with the *Allow* or *Deny* actions are temporarily allowed to access the network, so that no popup windows appear with questions about the network event.

12.5.6 Display settings

Remember the action for this application

Always enabled

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is activated as the default setting. This option is enabled as the default setting.

Always disabled

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is disabled as the default setting.

Allow signed application

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is automatically enabled during network access by signed applications. The manufacturers are: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Remember last used state

When this option is enabled, the option "Save action for this application" in the dialog box "Network event" is enabled in the same way as for the last network event. If the option "Save action for this application" of the dialog box "Network event" was enabled, this option is enabled for the following network event. If the option "Save action for this application" was disabled for the last network event, this option is also disabled for the following network event.

Show details

In this group of configuration options, you can setup the display of detailed information in the **Network event** window.

Show details on demand

If this option is enabled, the detailed information is only displayed in the*Network event* window on request, i.e. the detailed information is displayed by clicking on the **Show details** button in the *Network event* window.

Always show details

If this option is enabled, detailed information is always displayed in the *Network event* window.

Remember last used state

If this option is enabled, the display of detailed information is administered in the same way as for the previous network event. If detailed information was displayed or accessed during the last network event, detailed information is displayed for the following network event. If detailed information was hidden and not displayed during the last network event, detailed information is not displayed for the following network event.

Allow privileged

In this group of configuration options, you can define the status of the *Allow privileged* option in the **Network event** window.

Always enabled

If this option is enabled, the *Allow privileged* option is enabled as the default setting in the *Network event* window.

Always disabled

If this option is enabled, the *Allow privileged* option is disabled as the default setting in the *Network event* window.

Remember last used state

If this option is enabled, the status of the *Allow privileged* option is handled in the same way as for the previous network event in the *Network event* window: If the option *Allow privileged* was enabled for execution of the last network event, the option is enabled by default for the following network event. If the option *Allow privileged* was disabled for execution of the last network event, the option is disabled by default for the following network event.

12.6 WebGuard

The WebGuard section of the Configuration is responsible for the configuration of the WebGuard.

12.6.1 Scan

WebGuard protects you against viruses or malware that reaches your computer from web pages that you load on your web browser from the Internet. The *Scan* heading can be used to set the behavior of the WebGuard component.

Scan

Enable Webguard

If this option is enabled, the web pages you request using an Internet browser are scanned for viruses and malware. WebGuard monitors the data transferred from the Internet using the HTTP protocol at ports 80, 8080, 3128. If any affected web pages are detected, the loading of the web pages is blocked. If this option is disabled, the WebGuard service is still started, but the scan for viruses and malware is disabled.

Drive-by protection

Drive-by protection allows you to make settings to block I-Frames, also known as inline frames. I-Frames are HTML elements, i.e. elements of Internet pages that delimit an area of a web page. I-Frames can be used to load and display different web content - usually other URLs - as independent documents in a subwindow of the browser. I-Frames are mostly used for banner advertising. In some cases, I-Frames are used to conceal malware. In these cases the area of the I-Frame is mostly invisible or almost invisible in the browser. The *Block Suspect I-Frames* option allows you to check and block the loading of I-Frames.

Block suspicious I-frames

If this option is enabled, I-Frames on the web pages you request are scanned according to certain criteria. If there are suspect I-Frames on a requested web page, the I-Frame is blocked. An error message (HTTP status code 403) is displayed in the I-Frame window.

Default

If this option is enabled, I-Frames with suspect content is blocked.

Advanced

If this option is enabled, I-Frames with suspect content and I-Frames used in a suspicious way are blocked. The use of I-Frames is considered suspect if the I-Frame is very small and is therefore invisible or almost invisible in the browser of if the I-Frame is placed in an unusual position on the web page.

12.6.1.1. Action for concerning files

Action for concerning files

You can define the actions to be carried out by WebGuard when a virus or unwanted program is detected.

Interactive

If this option is enabled, a dialog window appears when a virus or unwanted program is detected during an on-demand scan, in which you can choose what is to be done with the affected file. This option is enabled as the default setting.

Permitted actions

In this display box you can specify those actions that are to be displayed in the dialog box in the event that a virus or unwanted program is detected. You must activate the corresponding options for this.

Refuse access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. WebGuard logs the detection to the report file if the report function is activated. WebGuard also appends an entry to the event log if the relevant option is enabled.

Quarantine

In the event of a virus or malware being detected, the website requested from the web server and/or the transferred data and files are moved into quarantine. The affected file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center.

ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by WebGuard to your web browser.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that is to be activated by default and click on the "Default" button.

Click here for more information.

Show progress bar

If this option is enabled, a desktop notification appears with a download progress bar if a download of website content exceeds a 20 second timeout. This desktop notification is designed in particular for downloading websites with larger data volumes: If you are surfing with WebGuard, website contents are not downloaded incrementally in the Internet browser, as they are scanned for viruses and malware before being displayed in the Internet browser. This option is disabled as the default setting.

Automatic

If this option is enabled, then no dialog box for selecting an action appears following the detection of a virus or unwanted program. WebGuard reacts according to the settings you define in this section.

Display detection alerts

If this option is activated, then for each detection of a virus or unwanted program a warning message appears showing the actions being executed.

Primary action

The primary action is the action carried out when WebGuard finds a virus or an unwanted program.

Deny access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. WebGuard logs the detection to the report file if the report function is activated. WebGuard also appends an entry to the event log if the relevant option is enabled.

isolate

In the event of a virus or malware being detected, the website requested from the web server and/or the transferred data and files are moved into quarantine. The affected file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center.

ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by WebGuard to your web browser. Access to the file is permitted and the file is ignored.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

12.6.1.2. Locked requests

In **Locked requests** you can specify the file types and MIME types (content types for the transferred data) to be blocked by WebGuard. The Web filter lets you block known phishing and malware URLs. WebGuard prevents the transfer of data from the Internet to your computer system.

File types / MIME types to be blocked by WebGuard (user-defined)

All file types and MIME types (content types for the transferred data) in the list are blocked by WebGuard.

Input box

In this box, enter the names of the MIME types and file types you want WebGuard to block. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. . **video/mpeg** or **audio/x-wav**.

Note
Files which are already stored on your computer system as temporary Internet files and blocked by WebGuard can however by downloaded locally from the Internet by your computer's Internet browser. Temporary Internet files are files saved on your computer by the Internet browser so that websites can be accessed more quickly

Note
The list of blocked file and MIME types is ignored if they are entered in the list of excluded file and MIME types under WebGuard::Scan::Exceptions.

Note
No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples: Excluded file and MIME types

- `application/octet-stream` = application/octet-stream MIME type files (executable files *.bin, *.exe, *.com, *dll, *.class) are blocked by WebGuard.
- `application/olescript` = application/olescript MIME type files (ActiveX script-files *.axs) are blocked by WebGuard.
- `.exe` = All files with the extension .exe (executable files) are blocked by WebGuard.
- `.msi` = All files with the extension .msi (Windows Installer files) are blocked by WebGuard.

Add

The button allows you to copy MIME and file types from the input field into the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Web-Filter

The Web filter is based on an internal database, updated daily, that classifies URLs according to content.

Activate web filter

When the option is enabled, all URLs matching the selected categories in the Web filter list are blocked.

Web filter list

In the Web filter list you can select the content categories whose URLs are to be blocked by WebGuard.

Note
The Web filter is ignored for entries in the list of excluded URLs under WebGuard::Scan::Exceptions.

Note
Spam URLs are URLs sent with spam emails. The Fraud and Deception category covers web pages with "Subscription Expires" and other offers of services whose costs are hidden by the provider.

12.6.1.3. Exceptions

These options allow you to set exceptions based on MIME types (content types for the transferred data) and file types for URLs (Internet addresses) for scanning by WebGuard. The MIME types and URLs specified are ignored by WebGuard, i.e. that data is not scanned for viruses and malware when it is transferred to your computer system.

MIME types skipped by WebGuard

In this field you can select the MIME types (content types for the transferred data) to be ignored by WebGuard during scanning.

File types/MIME types skipped by WebGuard (user-defined)

All MIME types (content types for the transferred data) in the list are ignored by WebGuard during scanning.

Input box

In this box you can input the name of the MIME types and file types to be ignored by WebGuard during scanning. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.

Note
No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

Warning
All file types and content types on the exclusion list are downloaded into the Internet browser without further scanning of the blocked access (List of file and MIME types to be blocked in WebGuard::Scan::Blocked access) or by WebGuard: For all entries on the exclusion list, the entries on the list of file and MIME types to be blocked are ignored. No scan for viruses and malware is carried out.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples: Excluded file and MIME types

- `audio/` = All audio media type files are excluded from WebGuard scans
- `video/quicktime` = All Quicktime sub-type video files (*.qt, *.mov) are excluded from WebGuard scans
- `.pdf` = All Adobe PDF files are excluded from WebGuard scans.

Add

The button allows you to copy MIME and file types from the input field into the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

URLs skipped by WebGuard

All URLs in this list are excluded from WebGuard scans.

Input box

Input box You can specify parts of the URL, using leading or concluding dots to indicate the domain level: .domainname.de for all pages and all subdomains of the domain. Indicate websites with any top-level domain (.com or .net) with a concluding dot: **domainname.**. If you indicate a string without a leading or concluding dot, the string is interpreted as a top-level domain, e.g. **net** for all NET-Domains (www.domain.net).

Note
You can also use the wildcard * for any number of characters when specifying URLs. You can also use leading or concluding dots in combination with wildcards to indicate the domain level:
.domainname.*
*.domainname.com
.*name*.com (valid but not recommended)
Specifications without dots, like *name*, are interpreted as part of a top-level domain and are not advisable.

Warning
All websites on the list of excluded URLs are downloaded into the Internet browser without further scanning by the web filter or WebGuard: For all entries in the list of excluded URLs, the entries in the web filter (see WebGuard::Scan::Blocked access) are ignored. No scan for viruses and malware is carried out. Only trusted URLs should therefore be excluded from WebGuard scans.

Add

The button allows you to copy the URL entered in the input field (Internet address) to the viewer window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Examples: Skipped URLs

- `www.avira.com` -OR- `www.avira.com/*`

  = All URLs with the domain 'www.avira.com' are excluded from WebGuard scans: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,..
  URLs with the domain 'www.avira.de' are not excluded from WebGuard scans.

- `avira.com` -OR- `*.avira.com`

  = All URLs with the second and top-level domain 'avira.com' are excluded from WebGuard scans: The specification implies all existing subdomains for '.avira.com': www.avira.com, forum.avira.com,...

- `avira.` -OR- `*.avira.*`

  = All URLs with the second-level domain 'avira' are excluded from WebGuard scans: The specification implies all existing top-level domains or subdomains for '.avira': www.avira.com, www.avira.de, forum.avira.com,...

- `.*domain*.*`

  All URLs containing a second-level domain with the string 'domain' are excluded from WebGuard scans: www.domain.com, www.new-domain.de, www.sample-domain1.de, ...

- `net` -OR- `*.net`

  = All URLs with the top-level domain 'net' are excluded from WebGuard scans: www.name1.net, www.name2.net,...

Warning
Enter the URLs you want to exclude from the WebGuard scan as precisely as possible. Avoid specifying an entire top-level domain or parts of a second-level domain because there is a risk that Internet pages that distribute malware and undesirable programs will be excluded from the WebGuard scan through global specifications under exclusions. You are recommended to specify at least the complete second-level domain and the top-level domain: domainname.com

12.6.1.4. Heuristic

This configuration section contains the settings for the heuristic of the Avira AntiVir Professional search engine.

Avira AntiVir Professional contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Avira AntiVir Professional contains a highly powerful macro virus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

enable AHeAD

Avira AntiVir Professional contains a very powerful heuristic in the form of AntiVir AheAD technology, which can also detect unknown (new) malware. If this option is activated, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira AntiVir Professional detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This setting is activated by default if you have selected the use of this heuristic.

High detection level

If this option is enabled, Avira AntiVir Professional detects much more unknown malware, however false positives can also be expected.

12.6.2 Report

The WebGuard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then WebGuard does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, WebGuard records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Advanced

If this option is enabled, WebGuard logs less important information to the report file as well.

Complete

If this option is enabled, WebGuard logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

12.7 Update

In the *Update* section you can configure the automatic receiving of updates and the connection to the download servers. You can specify various update intervals and activate or deactivate automatic updating.

Note
If you configure AntiVir Professional in the AntiVir Security Management Center, automatic updates are not available.

Automatic update

Activate

If this option is enabled, automatic updates are performed for the enabled events at the interval specified.

Automatic update every n days / hours / minutes

In this box you can specify the interval at which the automatic update is carried out. To change the update interval, highlight one of the time options in the box and change it using the arrow key to the right of the input box.

Start job while connecting to the Internet (dial-up)

If this option is enabled, in addition to the specified update interval, the update job is carried out every time an Internet connection is established.

Repeat job if the time has already expired

If this option is enabled, past update jobs are carried out that could not be carried out at the time specified, for example because the computer was switched off.

Download

via web server

The update is carried out via a web server using an HTTP connection. You can use a proprietary web server on the Internet or a web server on an intranet, which obtains the update files from a proprietary download server on the Internet.

Note
You can access further settings for updating via a web server under: Configuration :: General :: Update :: Web server .

via file server / shared folders

The update is carried out via a file server on an intranet which obtains the update files from a proprietary download server on the Internet.

Note
You can access further settings for updating via a file server under: Configuration :: General :: Update :: File server .

12.7.1 Product update

Under **Product update**, configure how product updates or the notification of available product updates are handled.

Product updates

Download and automatically install product updates

If this option is enabled, product updates are downloaded and automatically installed by the Update component as soon as they become available. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Download product updates. If a restart is necessary, install the update after the system restart, otherwise install it immediately.

If this option is enabled, product updates will be downloaded as soon as they become available. If no restart is necessary, the update is installed automatically after the update file is downloaded. If a product update requires you to restart your computer, it will be executed at the next user-controlled system reboot and not immediately after the download of the update file. This has the advantage that the restart is not carried out while users are working at their computers. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Notification when new product updates are available

If this option is enabled, you will be notified by email when new product updates become available. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server. You will receive notifications via a desktop popup window and via an alert from the Updater in the Control Centre under Overview::Events.

Notify again after n day(s)

If the product update was not installed after the initial notification, enter in this box the number of days that are to elapse before you are again notified that product updates are available.

Do not download product updates

If this option is enabled, no automatic product updates or notifications of available product updates by the Updater are carried out. Updates to the virus definition file and search engine are carried out independently of this setting.

Important
An update of the virus definition file and of the search engine is carried out during every update process independent of the settings for the product update (see chapter Updates).

Note
If you have enabled an option for an automatic product update, you can configure further restart notification and cancellation options under Restart settings.

12.7.2 Restart settings

When a product update is carried out by AntiVir Professional, you may have to restart your computer system. If you have selected automatic product updates under General::Update::Product update , you can choose between the different restart notification and restart cancellation options under **Restart settings**.

Note
Note that your restart settings allow you to choose between two options for executing a product update requiring a computer restart in the configuration under General::Update::Product update.

Automatic execution of the product update with the required computer restart when update is available: the update and the restart are carried out while users are working on their computers. If you have enabled this option, it may be useful to select restart routines with a cancel option or reminder function.

Execution of the product update where a computer restart is required after the next system reboot: the update and the restart are carried out after users have started up their computers and logged in. Automatic restart routines are recommended for this option..

Restart settings

Restart the computer after n seconds

If this option is enabled, the necessary restart is carried out **automatically** after a product update has been executed at the interval specified. A countdown message appears with no option for canceling the computer restart..

Reminder message for restart every n seconds

If this option is enabled, the necessary restart is **not** carried out automatically after a product update has been executed. At the interval specified, you will receive restart notifications without cancel options. These notifications let you confirm the computer restart or select **Remind me again** .

Query whether computer should be restarted

If this option is enabled, the necessary restart is **not** carried out automatically after a product update has been executed. You will receive one message in which you can confirm the restart or cancel the restart routine.

Restart computer without query

If this option is enabled, the necessary restart is carried out **automatically** after a product update has been executed. You will not receive any notification.

12.7.3 File server

In the case of more than one workstation in a network, Avira AntiVir Professional can download an update from a file server in the intranet, which in turn obtains the update files from a proprietary download server on the Internet. It can thus be ensured that the Avira AntiVir Professional is up to date on all workstations.

Note
The configuration section is only enabled if the option **Via file server / shared folders** has been selected under Configuration :: General :: Product update

Download

Enter the name of the file server on which the AntiVir Professional update files and the required directories '/release/update/' are located. The following must be specified: file://<IP address of the file server>/release/update/. The 'release' directory must be a directory that can be accessed by all users.

...

The button opens a window in which you can select the required download directory.

Server login

Login name

Enter your login name on the server.

Login password

Enter the relevant password for logging in on the server here. The characters entered are masked with *.

Note
If you do not specify any data in the Server login section, no authentication will be carried out when accessing the file server. In this case sufficient user rights must be available on the file server.

12.7.4 Web server

The update can be performed directly via a web server on the Internet or the intranet.

Web server connection

Use existing connection (network)

This setting is displayed if your connection is used via a network.

Use the following connection:

This setting is displayed if you define your connection individually.

The Updater automatically detects which connection options are available. Connection options which are not available are grayed out and cannot be activated. A dial-up connection can be established manually via a phone book entry in Windows, for example.

- **User:** Enter the user name of the selected account.
- **Password:** Enter the password for this account. For security, the actual characters you type in this space are replaced by asterisks (*).

Note
If you have forgotten an existing Internet account name or password, contact your Internet Service Provider.

Note
The automatic dial-up of the updater through so-called dial-up tools (e.g. SmartSurfer, Oleco, ...) is currently not available in Avira AntiVir Professional.

Terminate a dial-up connection that was set up for the update

If this option is enabled, the RDT connection made for the update is automatically interrupted again as soon as the download has been successfully carried out.

Note
This option is not available under Vista. Under Vista the dial-up connection opened for the update is always terminated as soon as the download has been carried out.

Download

Standard-Server

Enter the addresses (URL) of the web servers from which the updates and the required update directory 'update' are to be loaded. The format for the address of the web server is as follows: http://<address of the web server>[:Port]/update. If you do not specify a port, port 80 will be used. By default, the accessible web servers of Avira GmbH are specified for updating AntiVir Professional. You can, however, use your own web servers on the company intranet. If a number of web servers are specified, separate each one by a comma.

Default

The button restores the predefined addresses.

Priority server

In this field, enter the update directory and URL of the web server that will first be requested to provide the update. If this server cannot be reached, the standard servers indicated will be used. The format for the address of the web server is as follows: http://<address of web server>[:Port]/update. If you do not specify a port, port 80 will be used.

12.7.4.1. Proxy

Proxy server

Do not use a proxy server

If this option is enabled, your connection to the web server is not carried out via a proxy server.

Use Windows system settings

When the option is enabled, the current Windows system settings are used for the connection to the web server via a proxy server.

Use the following proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

Address

Please enter the URL or the IP address of the proxy server you should use to connect to the web server.

Port

Please enter the port number of the proxy server you should use to connect to the web server.

Login name

Enter your login name on the proxy server here.

Login password

Enter the relevant password for logging in on the proxy server here. For security, the actual characters you type in this space are replaced by asterisks (*).

Examples:

Address:	proyx.domain.com	Port:	8080
Address:	192.168.1.100	Port:	3128

12.8 General

12.8.1 Email

With certain events, Avira AntiVir Professional can send alerts and messages via email to one or more recipients. This is done with the Simple Message Transfer Protocol (SMTP).

The messages can be triggered by various events. The following components support email sending:

- Guard: Sending notifications
- Scanner: Sending notifications
- Updater: Sending notifications

Note
Please note that ESMTP is not supported. In addition, an encrypted transfer via TLS (Transport Layer Security) or SSL (Secure Sockets Layer) is currently not possible.

Email messages

SMTP Server

Enter the name of the host to be used here - either its IP address or the direct host name. The maximum possible length of the host name is 127 characters.

For example:

192.168.1.100 or mail.musterfirma.de.

Sender address

In this input box, enter the email address of the sender. The maximum length of the sender's address is 127 characters.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an email is sent. Avira AntiVir Professional can transmit alerts with authentication to the SMTP server via email.

Use authentication

If this option is enabled, a user name and a password can be entered in the relevant boxes for login (authentication).

- **User name**: Enter your user name here.
- **Password**: Enter the relevant password here. The password is saved in encrypted form. For security, the actual characters you type in this space are replaced by asterisks (*).

Send test email

When you click on the button, Avira AntiVir Professional attempts to send a test email to the sender address to check the data entered.

12.8.2 Extended threat categories

Selection of extended threat categories

Avira AntiVir Professional protects you against computer viruses.

In addition, you can scan according to the following extended threat categories.

- Backdoor Clients (BDC)
- Dialer (DIALER)
- Games (GAMES)

- Jokes (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Unusual runtime packers (PCK)
- Double Extension Files (HEUR-DBLEXT)
- Phishing
- Application (APPL)

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

Select all

If this option is enabled, all types are enabled.

Default values

This button restores the predefined default values.

Note
If a type is disabled, files recognized as being of the relevant program type are no longer indicated. No entry is made in the report file.

12.8.3 Password

You can protect Avira AntiVir Professional in different areas with a password. If a password has been issued, you will be asked for this password every time you want to open the protected area.

Password

Enter password

Enter your required password here. For security reasons, the actual characters you type in this space are replaced by asterisks (*). The password can only have a maximum of 20 chars. Once the password has been issued, the program refuses access if an incorrect password is entered. An empty box means "No password".

Confirm password

Confirm the password entered above by entering again here. For security, the actual characters you type in this space are replaced by asterisks (*).

Note
The password is case-sensitive!

Areas protected by password

Avira AntiVir Professional can protect individual errors with a password. By clicking on the relevant box, the password request can be disabled or reactivated for individual areas as required.

Password-protected area	Function
Control Center	If this option is enabled, a password is required to start the Control Center.

Activate / deactivate Guard	If this option is enabled, the pre-defined password is required to enable or disable AntiVir Guard.
Activate / deactivate MailGuard	If this option is enabled, the pre-defined password is required to enable/disable MailGuard.
Activate / deactivate Firewall	If this option is enabled, the pre-defined password is required to enable/disable the Firewall.
Activate / deactivate WebGuard	If this option is enabled, the pre-defined password is required to enable/disable WebGuard.
Add and modify jobs	If this option is enabled, a password is required when adding and changing jobs in the Scheduler.
Start product updates	If this option is enabled, a password is required to start the product update in the update menu.
Download rescue CD from the Internet	If this option is enabled, a password is required to start downloading the Avira Rescue CD.
Quarantine	If this option is enabled, all possible areas of the quarantine manager protected by a password are enabled. By clicking on the relevant box, the password enquiry can be disabled or enabled again on request for individual areas.
Restore affected objects	If this option is enabled, a password is required to restore an object.
Repair affected objects	If this option is enabled, a password is required to repair an object.
Affected object properties	If this option is enabled, a password is required to display the properties of an object.
Delete affected objects	If this option is enabled, a password is required to delete an object.
Send email to Avira	If this option is enabled, a password is required to send an object to the Avira Malware Research Center for examination.
Copying affected objects	If this option is enabled, a password is required to copy the affected object.
Configuration	If this option is enabled, configuration of Avira AntiVir Professional is only possible after entering the pre-defined password.

Manually switch configuration	If this option is enabled, a password will be required if you want to switch manually to a different configuration profile.
Enable expert mode	If this option is enabled, a password is required to enable expert mode.
Installation / Uninstallation	If this option is enabled, a password is required for installation or uninstallation of Avira AntiVir Professional.

12.8.4 Security

Update

Alert if last update older than n day(s)

In this box you can enter the maximum number of days allowed to have passed since the last update of Avira AntiVir Professional. If this number of days has passed, a red icon is displayed for the update status under Status in the Control Center.

Show notice if the virus definition file is out of date

If this option is enabled, you will obtain an alert message if the virus definition file is not up-to date. With the help of the alert option, you can configure the temporal interval for an alert message if the last update is older than n day(s).

Product protection

Protect processes from unwanted termination

If this option is enabled, all AntiVir Professional processes are protected against unwanted termination by viruses and malware or against 'uncontrolled' termination by a user e.g. via Task-Manager. This option is enabled as the default setting.

Advanced password protection

If this option is enabled, all AntiVir Professional processes are protected with advanced options from unwanted termination. Advanced password protection requires considerably more computer resources than simple password protection . That is why the option is disabled as the default setting. To enable this option, you have to restart your computer.

Important
Password protection is not available for Windows XP 64 Bit !

Warning
If process protection is enabled, interaction problems can occur with other software products. Disable process protection in these cases.

Protect files and registry entries from manipulation

If this option is enabled, all registry entries of AntiVir Professional and all program files (binary and configuration files) are protected from manipulation. Protection against manipulation entails preventing write, delete and, in some cases, read access to the registry entries or program files by users or external programs. To enable this option, you have to restart your computer.

Note
When this option is activated, changes can only be made to the configuration, including changes to scan or update requests, can only be made by means of the user interface.

Important
Protection for files and registration entries is not available for Windows XP 64 Bit !

12.8.5 WMI

Support for Windows Management Instrumentation

Windows Management Instrumentation is a basic Windows administration technique that uses script and programming languages to allow read and write access, both local and remote, to settings on Windows systems. AntiVir Professional supports WMI and provides data (status information, statistical data, reports, planned requests, etc.) as well as events and methods (stopping and starting processes) at an interface. WMI enables you to download operating data from AntiVir Professional and to control AntiVir Professional . You can request a complete reference guide to the WMI interface from the AntiVir Professional manufacturer. The reference file is available in PDF format when you sign a confidentiality agreement.

Enable WMI support

When this option is enabled, you can download operating data from AntiVir Professional via WMI.

Allow enabling/disabling of services

When this option is enabled, you can enable and disable services from AntiVir Professional via WMI.

12.8.6 Directories

Temporary path

In this input box, enter the path where Avira AntiVir Professional will store its temporary files.

Use default system settings

If this option is enabled, the settings of the system are used for handling temporary files.

Note
You can see where your system saves temporary files - for example with Windows XP - under: Start | Settings | Control Panel | System | Tab "Advanced" | Button "Environment Variables". The temporary variables (TEMP, TMP) for the currently registered user and for system variables (TEMP, TMP) are shown here with their relevant values.

Use following directory

If this option is enabled, the path displayed in the input box is used.

The button opens a window in which you can select the required temporary path.

Default

The button restores the pre-defined directory for the temporary path.

Report directory

This input box contains the path to the report file of Avira AntiVir Professional.

...

The button opens a window in which you can select the required directory.

Default

The button restores the pre-defined path to the report directory.

Quarantine directory

This box contains the path to the quarantine directory of Avira AntiVir Professional.

...

The button opens a window in which you can select the required directory.

Default

The button restores the predefined path to the quarantine directory.

12.8.7 Warnings

12.8.7.1. Network

You can send individually configurable alerts from the Scanner or from the Guard to any workstations in your network.

Note
Please check whether the "Message service" has been started. You will find the service (i.e. in Windows XP, for example) under "Start | Settings | System control | Administration | Services".

Note
An alert is always sent to computers, NOT to a certain user.

Warning
This functionality is no longer supported by the following operating systems:
Windows Server 2008 and higher
Windows Vista and higher

Send message to

The list in this window shows names of computers that receive a message when a virus or unwanted program is found.

Note
A computer can always be entered only once in this list.

Add

This button lets you add another computer. A window is opened in which you can enter the names of new computers. A computer name can be a maximum of 15 characters long.

The button opens a window in which you can alternatively select a computer directly from your computer environment.

Delete

This button lets you delete the currently selected entry from the list.

Guard

Network alerts

If this option is enabled, network alerts are sent. This option is disabled as the default setting.

Note
To enable this option, at least one recipient must be entered under General::Alerts::Network .

Message to be sent

The window shows the message sent to the selected workstation when a virus or unwanted program is detected. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combinations for formatting the message:

Strg + Tab	Inserts a tab. The current line is indented by several characters to the right.
Strg + Enter	inserts a line break.

The message can include wildcards for information which was found during the search. These wildcards are replaced by the actual text when sent.

The following wildcards can be used:

%VIRUS%	contains the name of the detected virus or of the unwanted program
%FILE%	contains the path and file name of the affected file
%COMPUTER%	contains the name of the computer on which the Guard is running
%NAME%	contains the name of the user who accessed the affected file
%ACTION%	contains the action carried out after the detection of the virus
%MACADDR%	contains the MAC address of the computer on which the Guard is running

Default

The button restores the predefined default text for an alert.

Scanner

Enable network alerts

If this option is enabled, network alerts are sent. This option is disabled as the default setting.

Note
To enable this option, at least one recipient must be entered under General::Alerts::Network .

Message to be sent

The window shows the message sent to the selected workstation when a virus or unwanted program is detected. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combinations for formatting the message:

Strg + Tab	Inserts a tab. The current line is indented by several characters to the right.
Strg + Enter	inserts a line break.

The message can include wildcards for information which was found during the search. These wildcards are replaced by the actual text when sent.

The following wildcards can be used:

%VIRUS%	contains the name of the detected virus or of the unwanted program
%NAME%	contains the name of the logged in user using the Scanner

Default

The button restores the predefined default text for an alert.

12.8.7.2. Email

Email

With certain events, Avira AntiVir Professional can send alerts and messages via email to one or more recipients. This is done with the Simple Message Transfer Protocol (SMTP).

The messages can be triggered by various events. The following components support email sending:

- Guard: Sending notifications
- Scanner: Sending notifications
- Updater: Sending notifications

Note
Please note that ESMTP is not supported. In addition, an encrypted transfer via TLS (Transport Layer Security) or SSL (Secure Sockets Layer) is currently not possible.

Email messages

SMTP Server

Enter the name of the host to be used here - either its IP address or the direct host name. The maximum possible length of the host name is 127 characters.

For example:

192.168.1.100 or mail.musterfirma.de.

Sender address

In this input box, enter the email address of the sender. The maximum length of the sender's address is 127 characters.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an email is sent. Avira AntiVir Professional can transmit alerts with authentication to the SMTP server via email.

Use authentication

If this option is enabled, a user name and a password can be entered in the relevant boxes for login (authentication).

- **User name**: Enter your user name here.
- **Password**: Enter the relevant password here. The password is saved in encrypted form. For security, the actual characters you type in this space are replaced by asterisks (*).

Send test email

When you click on the button, Avira AntiVir Professional attempts to send a test email to the sender address to check the data entered.

Guard

AntiVir Guard can send alerts by email to one or more recipients for certain events.

Guard

Email alerts

If this option is enabled, AntiVir Guard sends email messages with the most important information when a certain event occurs. This option is disabled as the default setting.

Email messages for the following events

The on-access scan detected a virus or unwanted program

If this option is enabled, you always receive an email with the name of the virus or unwanted program and the affected file when the on-access scan detects a virus or an unwanted program.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for an 'On-access detection' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

A critical error occurred in Guard

If this option is enabled, you receive an email if Avira AntiVir Professional detects an internal critical error.

Note
In this case, please inform our technical support and include the data given in the email. The specified file should also be sent for examination.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for a 'Critical error in Guard' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

Scanner

With certain events, the on-demand scan can send alerts and messages via email to one or more recipients.

Scanner

Enable email alerts

If this option is enabled, Avira AntiVir Professional sends email messages with the most important information when a certain event occurs. This option is disabled as the default setting.

Email messages for the following events

The on-demand scan detected a virus or unwanted program.

If this option is enabled, you receive an email with the name of the virus or unwanted program and the affected file whenever the on-demand scan detects a virus or an unwanted program.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for an 'Scan detection' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

End of scheduled scan.

When the option is activated, an email is sent when a scan job has been carried out. The email contains data on the point and duration of the scan job, on the folders and files scanned as well as on the viruses found and warnings.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for the 'End of scan' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

Add report file as attachment

If this option is enabled, the current report file of the Scanner component is added to the email as an attachment when sending Scanner notifications.

Recipient address(es)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

Updater

The Updater component can send notifications by email to one or more recipients for specific events.

Updater

Email alerts

If this option is enabled, the Update component sends email messages with the most important data when a specific event occurs. This option is disabled by default.

Email messages for the following events

No update necessary. Your program is up to date.

If this option is enabled, an email is sent if the Updater has successfully made a connection to the download server but there are no new files available on the server. This means that AntiVir Professional is up to date.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for a 'No update necessary' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

Update finished successfully. New files have been installed.

If this option is enabled, an email is sent for all updates carried out: This may be a product update or an update of the virus definition file or of the scanning engine.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for an 'Update successful – new files installed' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

Update finished successfully. A new product update is available.

If this option is enabled, an email is only sent if an update of the scanning engine or virus definition file was carried out without a product update, but a product update is available.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for an 'Update successful – product update available' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

Update failed.

If this option is enabled, an email is sent if the update has failed due to an error.

Edit

The*Edit* button opens the*Email template* window in which you can configure the notification for an 'Update failed' event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose (seeConfiguration::General::Email::Alerts::Email Template).

Add report file as attachment

If this option is enabled, the current report file of the Updater component is added to the email as an attachment when sending Updater notifications.

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

Note
Warning messages are always sent by email for the following events if a SMTP server and a recipient address have been configured for Updater notifications:
A product update is required for every further update of AntiVir Professional.
An update of the scanning engine or of the virus definition file could not be carried out as a product update is necessary.

These warning messages are sent irrespective of your email warning settings for the Update component.

Email template

In the*Email template* window you can configure the email notifications for the individual components to the enabled events . You can insert text of up to a maximum of 128 characters in the subject line and up to a maximum of 1024 characters in the message field.

The following variables can be used in the email subject and email message:

Globally acceptable variables

Variable	Value
Windows environment variables	The email notifications component supports all Windows environment variables.
%SYSTEM_IP%	IP address of the computer:
%FQDN%	Fully qualified domain name
%TIMESTAMP%	Event time stamp: Time and date format as per the language settings of the operating system
%COMPUTERNAME%	NetBIOS computer name
%USERNAME%	Name of user accessing the component
%PRODUCTVER%	Product version
%PRODUCTNAME%	Product name
%MODULENAME%	Name of the component sending the email
%MODULEVER%	Version of the component sending the email

Specific component variables

Variable	Value	Component emails
%ENGINEVER%	Version of search engine used	Guard Scanner
%VDFVER%	Version of virus definition file used	Guard Scanner
%SOURCE%	Fully qualified file name	Guard
%VIRUSNAME%	Name of the virus or unwanted program.	Guard
%ACTION%	Action carried out after the detection	Guard
%MACADDR%	MAC address of the first registered network card	Guard
%UPDFILESLIST%	List of updated files	Updater
%UPDATETYPE%	Update type: Update of search engine and virus definition file, or product update with update of search engine and virus definition file	Updater
%UPDATEURL%	URL of download server used for update	Updater
%UPDATE_ERROR%	Update error in words	Updater
%DIRCOUNT%	Number of scanned directories	Scanner
%FILECOUNT%	Number of files scanned	Scanner
%MALWARECOUNT%	Number of viruses or unwanted programs detected	Scanner
%REPAIREDCOUNT%	Number of infected files repaired	Scanner
%RENAMEDCOUNT%	Number of infected files renamed	Scanner
%DELETEDCOUNT%	Number of infected files deleted	Scanner
%WIPECOUNT%	Number of infected files overwritten and deleted	Scanner
%MOVEDCOUNT%	Number of infected files moved to quarantine	Scanner
%WARNINGCOUNT%	Number of warnings	Scanner
%ENDTYPE%	Status of scan: Terminated/Successfully completed	Scanner

%START_TIME%	Start time of the scan: Start time of the update	Scanner Updater
%END_TIME%	End of the scan End of the update	Scanner Updater
%TIME_TAKEN%	Duration of scan in minutes Duration of the update in minutes	Scanner Updater
%LOGFILEPATH%	Path and file name of the report file	Scanner Updater

12.8.7.3. Acoustic alerts

Acoustic alert

When a virus or malware is detected by the Scanner or Guard an acoustic alert is sounded in interactive action mode. You can now choose to activate or deactivate the acoustic alert and select an alternative wave file for the alert.

Note
The action mode of the Scanner is set in the configuration under Scanner::Scan::Action for concerning files. The action mode of the Guard is set in the configuration under Guard::Scan::Action for concerning files.

No warning

When this option is activated, there is no acoustic alert when a virus is detected by the Scanner or Guard.

Use PC speakers (only in interactive mode)

If this option is enabled, there is an acoustic alert with the default signal when a virus is detected by the Scanner or Guard. The acoustic alert is sounded on the PC's internal speaker.

Use the following Wave file (interactive mode only)

If this option is enabled, there is an acoustic alert with the selected Wave file when a virus is detected by the Scanner or Guard. The selected Wave file is played over a connected external speaker.

Wave file

In this input box you can enter the name and the associated path of an audio file of your choice. The default acoustic signal of AntiVir Professional is entered as standard.

...

The button opens a window in which you can select the required file with the aid of the file explorer.

Test

This button is used to test the selected wave file.

12.8.7.4. Warnings

AntiVir Professional generates so-called slide-ups, desktop notifications for specific events, which give information on successful or failed program sequences, such as updates. In *Warnings* you can enable or disable the notifications for specific events..

With desktop notifications, you have the option of disabling the notification directly in the slide-up. You can reverse the disabling of the notification in *Warnings*.

Warnings

on dial-up connections used

If this option is enabled, you will receive a desktop notification alert if a dialer creates a dial-up connection on your computer via the telephone or ISDN network. There is a danger that the connection may have been created by an unknown and unwanted dialer and that the connection may be chargeable. (see Viruses and more::Extended threat categories: Dialer).

on successfully updated files

If this option is enabled, you will receive a desktop notification whenever an update has been successfully performed and files updated.

on failed update

If this option is enabled, you will receive a desktop notification whenever an update fails: No connection to the download server could be created or the update files could not be installed.

that no update is necessary

If this option is enabled, you will receive a desktop notification whenever an update is started but installation of the files is not necessary as your program is up to date.

that you are logged on with administrator rights

If this option is enabled, when you log on to your computer, you will receive an alert if your user account includes administrator rights. For security reasons, it is recommended that you work with restricted user rights. By restricting the user rights with which you work on your computer, you prevent the automatic installation of unwanted programs and the unauthorized changing of system settings.

12.8.8 Events

Limit size of event database

Limit maximum number of events to n entries

If this option is enabled, the maximum number of events listed in the event database can be limited to a certain size; possible values: 100 to 10 000 entries. If the number of entered entries is exceeded, the oldest entries are deleted.

Delete events older than n day(s)

If this option is enabled, events listed in the event database are deleted after a certain period of time; possible values: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

Do not limit size of event database (delete events manually)

When this option has been activated, the size of the event database is not limited. However, a maximum of 20,000 entries are displayed in the program interface under Events.

12.8.9 Limit reports

Limit number of reports

Limit the number to n units

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

Delete all reports more than n day(s) old

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are: 1 to 90 days. This option is enabled by default with a value of 30 days.

Do not limit number of reports (manually delete reports)

If this option is enabled, the number of reports is not restricted.

Avira AntiVir Professional

www.avira.com

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com

AntiVir® is a registered trademark of the Avira GmbH. All other brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.

© Avira GmbH. All rights reserved.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q1-2010

AVIRA®